CA Enterprise Log Manager

Übersichtshandbuch

r12.1



CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

- CA Access Controll
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA® Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Security Compliance Manager (CA SCM)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- Überblick über den Schnellstart: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt nun über Syslogs hinaus Bezug auf weitere Ereignistypen, die vom Standardagenten auf dem CA Enterprise Log Manager-Server erfasst werden können.
- Alarme zu Richtlinienverletzungen: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt nun Bezug auf die Möglichkeit, Alarme als SNMP-Traps an Netzwerk-Sicherheitsüberwachungssysteme zu senden und einen IT PAM Ereignis-/Alarmausgabeprozess, z. B. zur Erstellung eines Help-Desk-Tickets, auszuführen.
- Bookshelf: Dieses bereits vorhandene Thema ist aktualisiert worden und nimmt Bezug auf das neue API-Programmierungshandbuch, das nun im CA Enterprise Log Manager-Bookshelf zur Verfügung steht.

Weitere Informationen

Überblick über den Schnellstart (siehe Seite 15)
Alarm bei Verletzung von Richtlinien (siehe Seite 56)
Überblick über das Bookshelf mit Dokumentation (siehe Seite 65)

Inhalt

Kapitel 1: Einführung

Dieses Kapitel enthält folgende Themen:

Über dieses Handbuch

Dieses *Übersichtshandbuch* bietet eine Einführung in CA Enterprise Log Manager. Es beginnt mit kurzen Lernprogrammen, die sofort eine praktische Einführung in das Produkt ermöglichen. Das erste Lernprogramm befasst sich mit der Einrichtung und Aktivierung eines Single-Server CA Enterprise Log Managers und dem Anzeigen von Syslogs, die von einem UNIX-Gerät in unmittelbarer Netzwerknähe erfasst wurden. Das zweite Lernprogramm gibt eine Einführung in die Installation eines Agents auf einem Windows-Betriebssystem, die Konfiguration der Protokollerfassung und die Anzeige daraus resultierender Ereignisprotokolle. Anschließend beschreibt es die Hauptfunktionen und gibt Hinweise zu weiteren Informationen. Dieses Handbuch richtet sich an alle Benutzer.

Zusammenfassung des Inhalts:

Abschnitt	Inhalt
Info zu CA Enterprise Log Manager	Integration von CA Enterprise Log Manager in Ihre aktuelle Netzwerkumgebung
Schnellstartbereitstellung	Installation eines Single-Server-Systems, Konfiguration von Syslog-Ereignisquellen, Update des Syslog-Connectors für den Standardagent und Anzeigen von verfeinerten Ereignissen
Bereitstellung von Windows-Agents	Vorbereiten der Agentinstallation, Installation eines Agents für das Windows-Betriebssystem, Konfiguration eines Connectors für die agentbasierte Erfassung, Aktualisieren der Ereignisquelle und Anzeigen generierter Ereignisse
Hauptfunktionen	Wichtige Funktionen nutzen, darunter die Protokollerfassung, die Protokollspeicherung, Konformitätsberichte und Alarme
Weitere Informationen zu CA Enterprise Log Manager	Weitere Informationen über Kurzinfos, die Online-Hilfe und das Dokumentations-Bookshelf

Hinweis: Weitere Informationen zu unterstützten Betriebssystemen oder zu den Systemanforderungen finden Sie in den *Versionshinweisen*. Schrittweise Anleitungen für die Installation von CA Enterprise Log Manager und die erste Konfiguration finden Sie im *Implementierungshandbuch.* Weitere Informationen zum Installieren eines Agents finden Sie im *Agent-Installationshandbuch*. Weitere Informationen zum Verwenden und Verwalten des Produkts finden Sie im *Verwaltungshandbuch.* Hilfe zum Verwenden einer CA Enterprise Log Manager-Seite finden Sie in der Online-Hilfe.

Info

Ziel von CA Enterprise Log Manager ist die IT-Konformität und -Sicherung. Es werden Informationen zur IT-Aktivität erfasst, standardisiert und aggregiert und entsprechende Berichte erstellt. Außerdem werden Alarme ausgegeben, wenn aufgrund einer möglichen Konformitätsverletzung Handlungsbedarf entsteht. Sie können Daten von unterschiedlichen sicherheits- und nicht sicherheitsbezogenen Geräten sammeln.

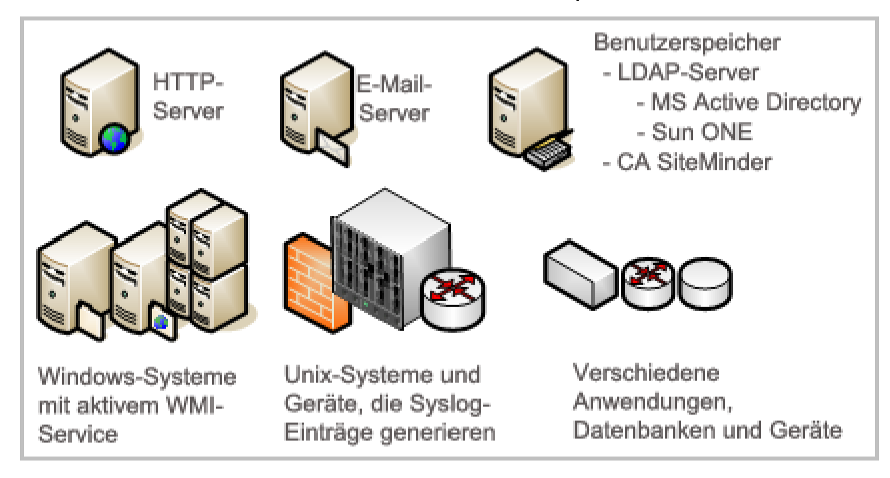
Ihr Netzwerk vor der Installation

Lokale Bestimmungen und Richtlinien schreiben die Aufbewahrung von Protokolldatensätzen vor. Zur Erfüllung dieser Vorgaben müssen Sie:

- Protokolle für Auditing-Zwecke verfügbar machen
- Protokolle über Jahre hinweg speichern
- Protokolle auf Anforderung wiederherstellen

Erschwerend für die Verwaltung von Protokolldatensätzen sind ihre große Anzahl, ihr Speicherort und ihre temporäre Natur. Protokolle werden durch Benutzer- und Prozessaktivitäten in der Software ständig generiert. Die Generierungsrate wird in Ereignissen pro Sekunde (EPS) gemessen. Für jedes aktive System, jede aktive Datenbank und jede aktive Anwendung in Ihrem Netzwerk werden Rohereignisse erfasst. An jeder Ereignisquelle müssen Ereignisprotokolle für die Speicherung gesichert werden, bevor sie überschrieben werden. Die Wiederherstellung von Ereignisprotokollen gestaltet sich schwierig, wenn Sicherungen aus anderen Ereignisquellen separat gespeichert werden.

Die Auswertung von Rohereignissen wird durch das Zeichenfolgenformat erschwert, bei dem der Ereignisschweregrad nicht hervorgehoben ist. Zudem variieren ähnliche Daten aus verschiedenen Systemen.



Ein optimaler Betrieb erfordert eine Lösung, in der sämtliche Protokolle konsolidiert werden, und die dafür sorgt, dass Protokolle gut lesbar sind, dass die Archivierung im Speicher automatisiert ist und die Protokollwiederherstellung vereinfacht wird. CA Enterprise Log Manager bietet diese Vorteile und gibt Ihnen die Möglichkeit, Alarme an Benutzer und Systeme zu senden, wenn kritische Ereignisse eintreten.

Installationsumfang

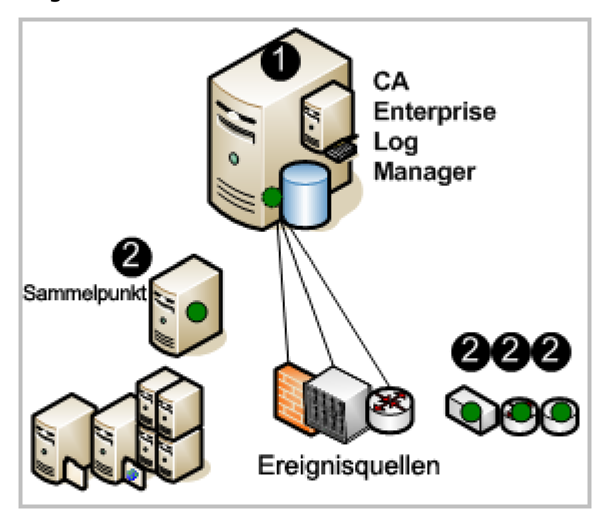
Es nimmt nur wenig Zeit in Anspruch, eine Single-Server-Lösung einzurichten und mit dem Erfassen von Ereignissen zu beginnen.

Die Installationsdatenträger enthalten folgende Komponenten:

- Betriebssystem (Red Hat Enterprise Linux) für die Soft-Appliance
- CA Enterprise Log Manager-Server
- CA Enterprise Log Manager-Agent (in dieser Dokumentation der Agent)

In der folgenden Abbildung ist CA Enterprise Log Manager ein Server, bestehend aus einem kleinen Server, einem dunklen (grünen) Kreis und einer Datenbank. Der kleine Server steht für das lokale Repository, das den Inhalt auf Anwendungsebene speichert. Der dunkle Kreis steht für den Standardagent, und die Datenbank steht für den Ereignisprotokollspeicher, in dem eingehende Ereignisprotokolle verarbeitet und für Abfragen und Berichte verfügbar gemacht werden.

Die dunklen (grünen) Kreise am Sammelpunkt und den anderen Ereignisquellen stehen für separat installierte Agents. Das Installieren von Agents ist optional. Mit dem Standardagent können Sie Syslogs von UNIX-kompatiblen Ereignissen erfassen, nachdem die erforderliche Konfiguration abgeschlossen ist.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Installieren Sie das Betriebssystem für die Soft-Appliance und anschließend die CA Enterprise Log Manager-Anwendung. Sobald Sie die Quellen konfiguriert haben, um Syslogs an CA Enterprise Log Manager auszugeben und die Syslog-Ziele in der Konfiguration des Connectors des Standardagents angegeben haben, werden Syslogs erfasst und zur leichteren Interpretation verfeinert.
2. (Optional) Sie können einen Agent auf einem Host installieren, den Sie als Sammelpunkt bestimmt haben, oder Sie können Agents direkt auf den Hosts mit Quellen, zu erfassende Ereignisse generieren, installieren.

Hinweis: Weitere Informationen zum Installieren der Soft-Appliance finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Installieren von Agents finden Sie im *Agent-Installationshandbuch*.

Weitere Informationen:

Installation eines Single-Server-Systems (siehe Seite 16)
Installieren eines Agents (siehe Seite 39)

Kapitel 2: Schnellstartbereitstellung

Dieses Kapitel enthält folgende Themen:

Überblick über den Schnellstart

Sie können eine einfache, funktionsfähige CA Enterprise Log Manager-Bereitstellung mit einer Soft-Appliance erstellen. Mit Hilfe des vordefinierten Syslog-Connectors kann der Standardagent generierte Syslog-Ereignisse empfangen. Sie müssen lediglich Ihre Syslog-Quellen konfigurieren, um Syslog-Ereignisse an CA Enterprise Log Manager weiterzugeben, und die Syslog-Connector-Konfiguration bearbeiten, so dass die Syslog-Ziele erkannt werden. Die Bandbreite zwischen dem Server und den Syslog-Quellen sowie die Latenz bestimmen, was empfangen wird.

Protokollsensoren, einschließlich WinRM und ODBC, unterstützen die direkte Protokollerfassung von über zwanzig Nicht-Syslog-Ereignisquellen. Der WinRM-Protokollsensor ermöglicht die direkte Ereigniserfassung von Servern, auf denen Windows-Betriebssysteme ausgeführt werden, wie z. B. Forefront Security für Exchange-Server, Forefront Security für SharePoint-Server, Microsoft Office Communication Server und der virtuelle Server Hyper-V, sowie Services wie Active Directory Certificate Services. Der ODBC-Protokollsensor ermöglicht, von Oracle9i- oder SQL Server 2005-Datenbanken generierte Ereignisse zu erfassen. Einzelheiten hierzu finden Sie in der CA Enterprise Log Manager-Produktintegrationsmatrix.

Sie benötigen für die Installation von CA Enterprise Log Manager die EiamAdmin-Anmeldeinformationen. Als EiamAdmin-Superuser konfigurieren Sie ein Administratorkonto, das Sie für die Konfiguration verwenden. Wenn Sie sich mit den Administrator-Anmeldeinformationen anmelden, können Sie überprüfen, ob das Setup funktionsfähig ist, indem Sie die selbstüberwachenden Ereignisse anzeigen.

Installation eines Single-Server-Systems

Ein Single-Server-System ist die einfachste Art, abgefragte Ereignisse anzuzeigen. Stellen Sie sicher, dass Sie ein Gerät wählen, das die minimalen Hardwareanforderungen für eine CA Enterprise Log Manager-Soft-Appliance erfüllt oder übertrifft.

Hinweis: Die zertifizierte Hardwareliste, Informationen zur Unterstützung von Betriebssystemen und zur Systemsoftware sowie Dienstanforderungen finden Sie in den *Versionshinweisen*.

So installieren Sie einen CA Enterprise Log Manager für ein Single-Server-System:

1. Halten Sie die folgenden Informationen bereit:
   - Ein Kennwort, das als Stammkennwort verwendet wird.
   - Hostname für Ihre Anwendung
   - Wenn DHCP nicht verwendet wird, die statische IP-Adresse, Subnet-Maske und Standard-Gateway für Ihre Anwendung
   - Domäne der Anwendung

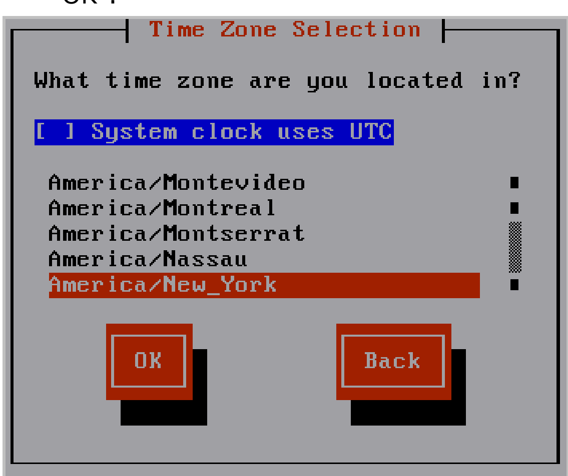
     Hinweis: Die Domäne muss auf den DNS-Servern in Ihrem Netzwerk registriert werden, um die Installation abzuschließen.
   - IP-Adressen der DNS-Server
   - (Optional) IP-Adresse des NTP-Zeitservers
   - Ein Kennwort für den Standard-Superuser-Installationsnamen "EiamAdmin"
   - CAELM.

     Dies ist der Standardanwendungsname für die CA Enterprise Log Manager-Anwendung.

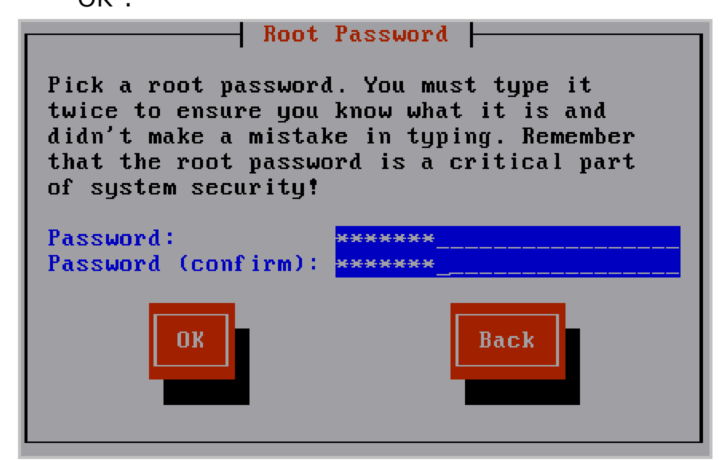
2. Installieren Sie das vorkonfigurierte Betriebssystem über den Datenträger, den Sie aus dem CA Enterprise Log Manager-Downloadpaket erstellt haben. Gehen Sie bei der Installation des Betriebssystems folgendermaßen vor:

   a. Wählen Sie einen Tastaturtyp aus. Der Standard ist USA.

   b. Wählen Sie eine Zeitzone (z. B. Amerika/New York), und wählen Sie "OK".



   c. Geben Sie das Kennwort ein, das als Stammkennwort verwendet werden soll. Geben Sie es erneut ein, um es zu bestätigen. Wählen Sie "OK".



Der Installationsfortschritt wird angezeigt.

d. Entnehmen Sie den Installationsdatenträger für das Betriebssystem, und drücken Sie die Eingabetaste, um das System neu zu starten.



Das System wird neu gestartet und wechselt in den nicht interaktiven Startmodus. Es werden Meldungen zum Installationsfortschritt angezeigt. Weitere Informationen zu dieser Installation werden in der folgenden Datei gespeichert: /tmp/pre-install_ca-elm.log.

Die folgende Eingabeaufforderung wird angezeigt:

Legen Sie den Datenträger "CA Enterprise Log Manager r12" für die Anwendungsinstallation ein, und drücken Sie die Eingabetaste.

3. Legen Sie den Datenträger der CA Enterprise Log Manager-Anwendung ein. Drücken Sie die Eingabetaste.

   Es wird überprüft, ob Ihr System die empfohlenen Mindestanforderungen für eine optimale Leistung erfüllt. Ist dies nicht der Fall, wird eine Meldung eingeblendet, in der Sie gefragt werden, ob Sie den Installationsprozess abbrechen möchten.

   Die folgende Eingabeaufforderung wird angezeigt:

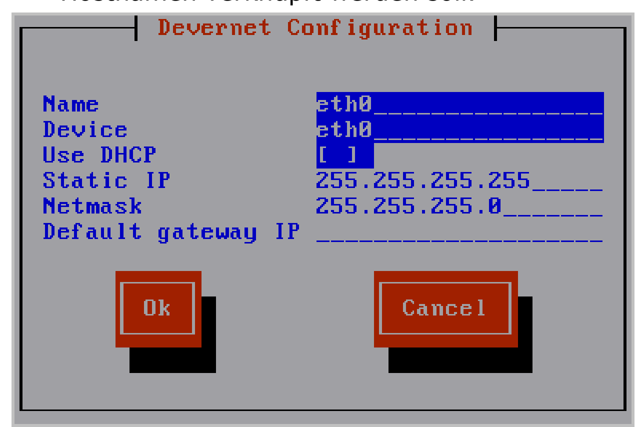
   Geben Sie einen neuen Hostnamen ein.

4. Geben Sie den Hostnamen für diese CA Enterprise Log Manager-Soft-Appliance ein. Geben Sie beispielsweise CALM1 ein.

5. Übernehmen Sie das Standardgerät "eth0". Drücken Sie die Eingabetaste, um zum nächsten Bildschirm zu wechseln.



6. Führen Sie einen der folgenden Schritte aus, und wählen Sie dann OK.
   - Wählen Sie "DHCP verwenden". Diese Option wird nur von Standalone-Testsystemen akzeptiert.
   - Geben Sie die statische IP-Adresse, die Subnet-Maske und eine Standard-Gateway-IP-Adresse ein, die mit dem eingegebenen Hostnamen verknüpft werden soll.



   Die Netzwerkservices werden mit den neuen, angezeigten Einstellungen neu gestartet.

   Die folgende Meldung wird angezeigt:

   Möchten Sie die Netzwerkkonfiguration ändern? (n):

7. Überprüfen Sie die Netzwerkeinstellungen. Wenn Sie zufrieden sind, geben Sie n ein oder drücken Sie die Eingabetaste, wenn die Meldung angezeigt wird, in der Sie die Netzwerkeinstellungen ändern können.

   Die folgende Meldung wird angezeigt:

   Geben Sie den Domänennamen für dieses System ein:

8. Geben Sie Ihren Domänennamen ein, z. B. <ihrunternehmen>.com.

   Die folgende Meldung wird angezeigt:

   Geben Sie eine kommagetrennte Liste mit DNS-Servern ein, die verwendet werden können:

9. Geben Sie die IP-Adressen Ihrer internen DNS-Server ein. Sie müssen durch Kommas ohne Leerzeichen voneinander getrennt sein.

   Systemdatum und -zeit werden in der folgenden Meldung angezeigt:

   Möchten Sie Systemdatum und -zeit ändern? (n)

10. Überprüfen Sie das angezeigte Systemdatum und die Systemzeit. Wenn Sie zufrieden sind, drücken Sie die Eingabetaste oder geben Sie n ein.

    Die folgende Meldung wird angezeigt:

    Möchten Sie das System konfigurieren, um die Uhrzeit über NTP zu aktualisieren?

11. Wenn Sie einen NTP-Server (Network Time Protocol) verwenden, gehen Sie wie folgt vor. Wählen Sie andernfalls "Nein", und fahren Sie mit dem nächsten Schritt fort.

    a. Wählen Sie für diese Meldung "Ja".

       Wenn Sie "Ja" wählen, wird die folgende Meldung angezeigt:

       Geben Sie den Namen oder die IP-Adresse des NTP-Servers an.

    b. Geben Sie den Hostnamen oder die IP-Adresse des NTP-Servers ein.

       Es wird eine Bestätigungsmeldung mit dem ungefähren Wortlaut angezeigt: "Ihr System wurde so konfiguriert, dass die Uhrzeit um Mitternacht über den NTP-Server unter <ihrntpserver> aktualisiert wird."

12. Lesen Sie die angegebenen Endbenutzerlizenzverträge (End User License Agreements oder EULAs), und gehen Sie folgendermaßen vor:

    a. Lesen Sie die EULA für das Sun Java Development Kit (JDK).

       Am Ende der EULA wird die folgende Meldung angezeigt:

       Stimmen Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zu? [Ja oder Nein]

    b. Geben Sie "Ja" ein, wenn Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zustimmen.

       Die Produktregistrierungsinformationen werden angezeigt, gefolgt von dieser Meldung:

       Drücken Sie zum Fortfahren die Eingabetaste.

    c. Drücken Sie die Eingabetaste.

       Die folgenden Meldungen geben an, dass zur Vorbereitung der CA Enterprise Log Manager-Installation die Systemeinstellungen konfiguriert werden. Der CA-Endbenutzer-Lizenzvertrag (EULA) wird angezeigt.

    d. Lesen Sie die CA EULA.

       Am Ende des Lizenzvertrags wird die folgende Meldung angezeigt:

       Stimmen Sie den Bestimmungen des oben aufgeführten Lizenzvertrags zu? [Ja oder Nein]:

    e. Geben Sie "Ja" ein, wenn Sie den Bestimmungen des Lizenzvertrags zustimmen.

       Die CA EEM-Serverinformationen werden angezeigt.

13. Befolgen Sie die folgenden Eingabeaufforderungen, um CA EEM zu konfigurieren.

    Verwenden Sie einen lokalen oder einen Remote-EEM-Server?
    Geben Sie l (lokal) oder r (remote) ein:

    a. Um ein Standalone-Testsystem zu erstellen, geben Sie l für "lokal" ein.

       Geben Sie das Kennwort für den Benutzer "EiamAdmin" des EEM-Servers ein:
       Bestätigen Sie das Kennwort für den Benutzer "EiamAdmin" des EEM-Servers:

    b. Geben Sie das Kennwort ein, das Sie dem EiamAdmin-Standard-Superuser zugewiesen haben, und bestätigen Sie es durch erneute Eingabe.

       Geben Sie einen Anwendungsnamen für diesen CAELM-Server (CAELM) ein:

    c. Drücken Sie die Eingabetaste, um CAELM zu akzeptieren, den Standardanwendungsnamen für CA Enterprise Log Manager.

       Die bisher eingegebenen EEM-Serverinformationen werden mit einer Meldung eingeblendet, in der Sie gefragt werden, ob Sie Änderungen vornehmen möchten.

```
EEM server is not installed on the local host.

EEM Server Information:
EEM Server Type - l (local) or r (remote): l
EEM Server Name: CALM1
EEM application name for this CAELM server: CAELM
Do you want to change the EEM Server information? (n): _
```

    d. Drücken Sie die Eingabetaste oder geben Sie "n" für "Nein" ein, um die eingegebenen CA EEM-Serverinformationen zu akzeptieren.

    Der Installationsvorgang wird gestartet. Die folgenden Meldungen zeigen den erfolgreichen Fortschritt der einzelnen CA Enterprise Log Manager-Komponenten, den Abschluss der Registrierungen, den Empfang von Zertifikaten, den Import von Dateien und die Konfiguration der Komponenten. Die folgende Meldung bestätigt, dass die CA ELM-Installation erfolgreich abgeschlossen wurde. Nach Abschluss der Installation zeigt das System die Anmeldeadresse der Konsole an.

14. Notieren Sie sich diese Adresse. Diese Adresse müssen Sie in einem Browser eingeben, um auf diesen CA Enterprise Log Manager-Server zuzugreifen. Diese lautet https://<hostname>:5250/spin/calm.

    Es wird eine Anmeldeaufforderung für den <hostname> angezeigt. Diese können Sie außer Acht lassen.

    Hinweis: Wenn Sie von dieser Anmeldeaufforderung aus die Eingabeaufforderung des Betriebssystems anzeigen möchten, geben Sie "caelmadmin" und das Standardkennwort ein, d. h. das Kennwort, das Sie dem Benutzerkonto für "EiamAdmin" zugewiesen haben. Mit diesem caelmadmin-Konto können Sie sich bei der Anwendung auf der Konsole oder über SSH anmelden.

15. Fahren Sie wie folgt fort:

    - Wenn Sie eine statische IP-Adresse konfiguriert haben, müssen Sie die IP-Adresse mit den in Schritt 9 festgelegten DNS-Servern registrieren.
    - Wenn Sie DHCP konfiguriert haben, aktualisieren Sie Ihre Hostdatei auf dem Gerät, von dem aus Sie über einen Browser auf diesen Server zugreifen möchten.
    - Gehen Sie zu der URL, die Sie in Schritt 14 notiert haben, und konfigurieren Sie den ersten Administrator.

Aktualisieren der Windows-Hostdatei

Während der Installation von CA Enterprise Log Manager können Sie einen oder mehrere DNS-Server festlegen oder DHCP wählen. Wenn Sie DHCP gewählt haben, müssen Sie Ihre Windows-Hostdatei auf dem Computer aktualisieren, über den Sie mit Ihrem Browser auf CA Enterprise Log Manager zugreifen möchten.

So aktualisieren Sie Ihre Hostdatei auf dem Host mit Ihrem Browser:

1. Öffnen Sie den Windows Explorer, und navigieren Sie zu C:\WINDOWS\system32\drivers\etc.
2. Öffnen Sie die Hostdatei mit einem Editor, z. B. Notepad.
3. Fügen Sie einen Eintrag mit der IP-Adresse des CA Enterprise Log Manager-Servers und den entsprechenden Hostnamen hinzu.
4. Wählen Sie im Menü "Datei" die Option "Speichern", und schließen Sie die Datei anschließend.

Konfigurieren des ersten Administrators

Nach der Installation eines Single-Server-CA Enterprise Log Manager bereiten Sie die Konfiguration vor, indem Sie die URL von CA Enterprise Log Manager von einer Remote-Workstation aus aufrufen, sich anmelden und ein Administratorkonto erstellen, mit dem Sie die Konfiguration vornehmen können.

Hinweis: Für diese Schnellstartbereitstellung werden der Standardbenutzerspeicher und die Standardkennwortrichtlinien akzeptiert. Normalerweise werden diese konfiguriert, bevor der erste Administrator hinzugefügt wird.

So konfigurieren Sie den ersten Administrator:

1. Öffnen Sie in Ihrem Browser die folgende URL, wobei der Hostname entweder aus dem Hostnamen oder der IP-Adresse des Servers besteht, auf dem Sie CA Enterprise Log Manager installiert haben.

   https://<hostname>:5250/spin/calm

2. Falls ein Sicherheitsalarm eingeblendet wird, gehen Sie folgendermaßen vor:

   a. Klicken Sie auf "Zertifikat anzeigen".

   b. Klicken Sie auf "Zertifikat installieren", übernehmen Sie die Standardeinstellungen, und schließen Sie den Import-Assistenten ab.

      Es wird eine Sicherheitswarnung eingeblendet, die Sie darauf hinweist, dass Sie ein Zertifikat installieren, das vorgibt, den Hostnamen des CA Enterprise Log Manager-Servers zu repräsentieren.

   c. Klicken Sie auf "Ja".

      Das Stammzertifikat wird installiert, und es wird eine Meldung eingeblendet, dass der Import erfolgreich war.

   d. Klicken Sie auf "OK".

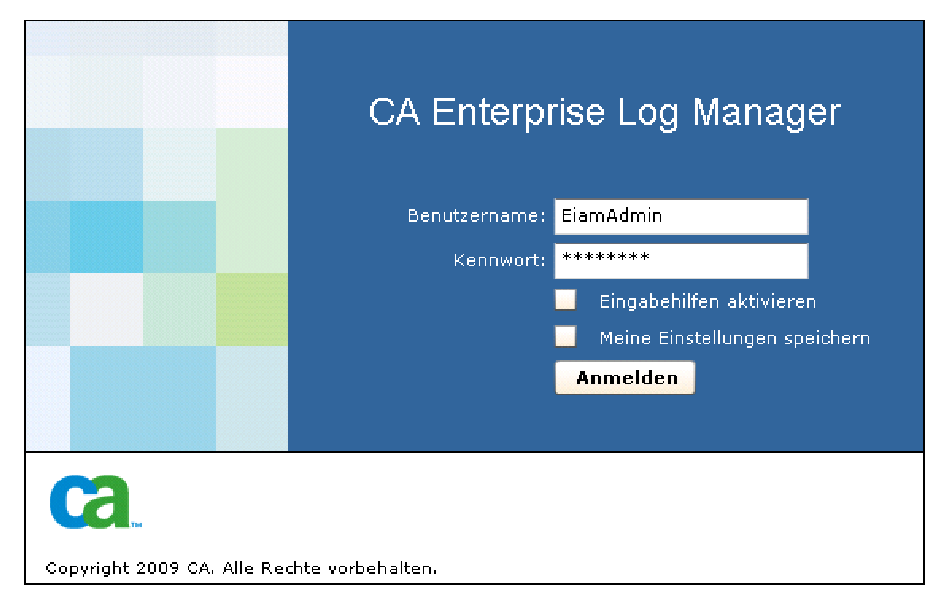
      Das Dialogfeld "Vertrauenswürdige Zertifikate" wird angezeigt.

   e. (Optional) Klicken Sie auf den Pfad des Zertifikats, und stellen Sie sicher, dass der Zertifikatstatus "OK" lautet.

   f. Klicken Sie auf "OK" und anschließend auf "Ja".

      Die Anmeldeseite wird angezeigt.

3. Melden Sie sich mit dem Benutzernamen "EiamAdmin" und dem Kennwort an, das Sie bei der Installation der Software verwendet haben. Klicken Sie auf "Anmelden".

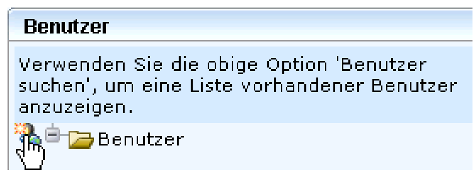


Die Anwendung wird mit der Administrator-Registerkarte und aktiver Unterregisterkarte für die Benutzer- und Zugriffsverwaltung geöffnet.

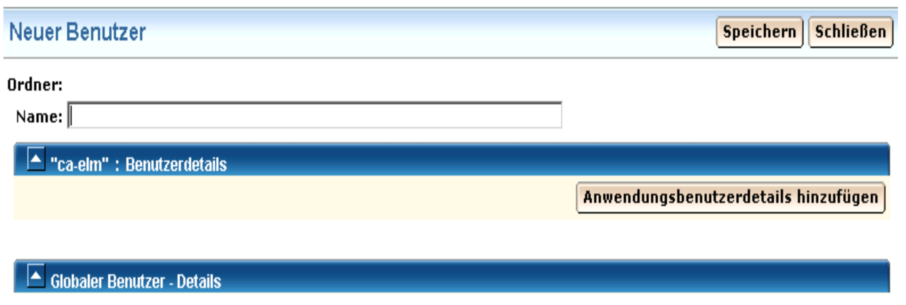
4. Klicken Sie auf "Benutzer".



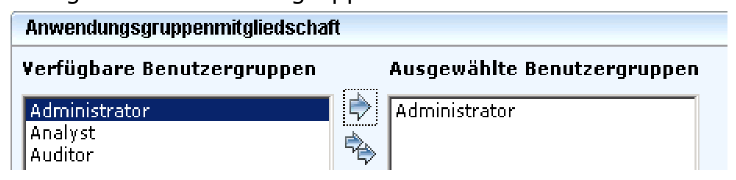
5. Klicken Sie auf "Neuen Benutzer hinzufügen".



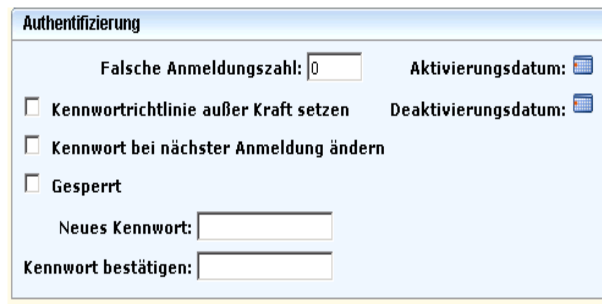
6. Geben Sie Ihren Namen in das Feld "Name" ein, und klicken Sie auf "Anwendungsbenutzerdetails hinzufügen".



7. Wählen Sie "Administrator", und verschieben Sie ihn in die Liste "Ausgewählte Benutzergruppen".



8. Geben Sie unter "Authentifizierung" in den beiden Feldern für Eingabe und Bestätigung ein Kennwort für das neue Konto ein.



9. Klicken Sie auf "Speichern" und anschließend auf "Schließen". Klicken Sie auf "Schließen".

10. Klicken Sie in der Symbolleiste auf "Abmelden".

    Die Anmeldeseite wird angezeigt.

11. Melden Sie sich mit den gerade definierten Administratoranmeldeinformationen erneut bei CA Enterprise Log Manager an.

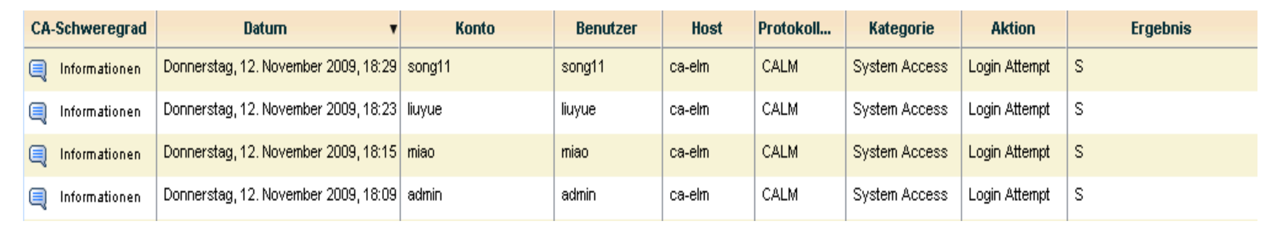
    CA Enterprise Log Manager wird geöffnet. Nun stehen alle Funktionen zur Verfügung. Die Registerkarte "Abfragen und Berichte" wird mit der untergeordneten Registerkarte "Abfragen" angezeigt.

12. (Optional) Zeigen Sie Ihre Anmeldeversuche wie folgt an:

    a. Wählen Sie in der Abfragekennungsliste den Eintrag "Systemzugriff".

    b. Wählen Sie in der Abfragekennungsliste den Eintrag "Systemzugriff - Details".

    Das Abfrageergebnis zeigt Ihre beiden Anmeldeversuche an, zuerst als "EiamAdmin", dann mit Ihrem Administratornamen. Beide Anmeldeversuche sind mit S für "Successful" (Erfolgreich) markiert.



CA-Schweregrad	Datum	Konto	Benutzer	Host	Protokoll...	Kategorie	Aktion	Ergebnis
Informationen	Donnerstag, 12. November 2009, 18:29	song11	song11	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:23	liuyue	liuyue	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:15	miao	miao	ca-elm	CALM	System Access	Login Attempt	S
Informationen	Donnerstag, 12. November 2009, 18:09	admin	admin	ca-elm	CALM	System Access	Login Attempt	S

Weitere Informationen:

Installation eines Single-Server-Systems (siehe Seite 16)

Konfigurieren von Syslog-Ereignisquellen

Um die direkte Erfassung von Syslog-Ereignissen durch den Standardagent zu ermöglichen, der auf jedem CA Enterprise Log Manager-Server existiert, müssen Sie zunächst die Syslog-Ereignisquellen definieren, über die Sie Ereignisse erfassen möchten, und die damit verbundene Integration festlegen. Anschließend führen Sie die beiden folgenden Schritte in beliebiger Reihenfolge durch:

- Konfigurieren Sie die Syslog-Ereignisquellen. Melden Sie sich bei den Hosts an, auf denen eine Syslog-Ereignisquelle ausgeführt wird, und konfigurieren Sie sie wie im Connector-Handbuch für diese Syslog-Integration beschrieben.
- Konfigurieren Sie den Syslog-Connector auf dem Standardagent, um Ziel-Syslog-Integrationen hinzuzufügen, die mit den konfigurierten Ereignisquellen verknüpft sind.

Sobald Sie diese beiden Konfigurationsschritte abgeschlossen haben, beginnt die Erfassung und Verfeinerung der Ereignisse. Dann können Sie CA Enterprise Log Manager verwenden, um im Standardformat für Sie wichtige Ereignisse anzuzeigen oder entsprechende Berichte zu erstellen. Sie können auch Alarme generieren, wenn bestimmte Ereignisse eintreten.

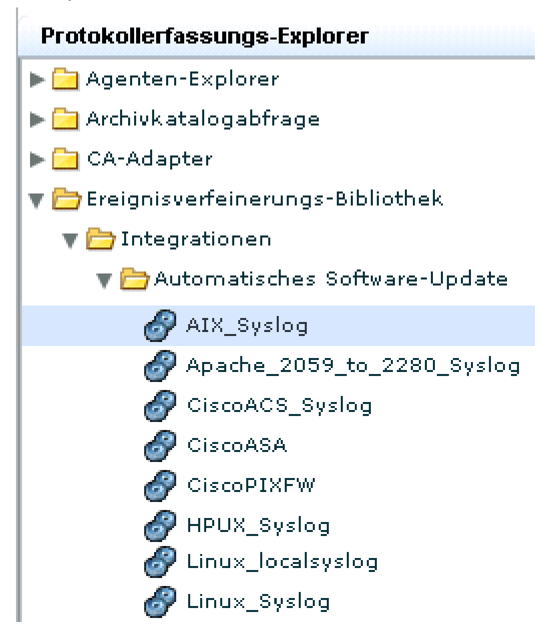
So konfigurieren Sie eine ausgewählte Syslog-Ereignisquelle:

1. Melden Sie sich bei dem Host an, auf dem sich eine Ziel-Syslog-Ereignisquelle befindet.
2. Starten Sie CA Enterprise Log Manager über einen Browser auf diesem Host.
3. Klicken Sie auf die Registerkarte "Verwaltung" und die untergeordnete Registerkarte "Protokollerfassung".

   Der Protokollerfassungs-Explorer wird geöffnet.

4. Erweitern Sie die Punkte "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatische Software-Updates".

   Eine Liste vordefinierter Integrationen wird angezeigt. Eine kurzes Beispiel:



5. Wählen Sie die Integration für die Ereignisquelle, die Sie konfigurieren müssen. Wenn Sie beispielsweise Syslogs erfassen möchten, die von einem AIX-Betriebssystem generiert wurden, müssen Sie "AIX_Syslog" wählen.

   Das Fenster "Integrationsdetails" wird angezeigt.



6. Klicken Sie auf die Schaltfläche "Hilfe" über dem Integrationsnamen im rechten Fensterbereich.

   Das Connector-Handbuch für die ausgewählte Integration wird angezeigt.

7. Klicken Sie auf den Bereich in den Konfigurationsanforderungen der Ereignisquelle. In diesem Beispiel wird beschrieben, wie Sie die Ereignisquelle des AIX-Betriebssystems konfigurieren, damit die Syslogs an CA Enterprise Log Manager gesendet werden.

Beispiel: Alternative Quelle für Connector-Handbücher: Support Online

Sie können ein ausgewähltes Connector-Handbuch über die CA Enterprise Log Manager-Benutzeroberfläche oder über den CA Support Online öffnen. Das folgende Beispiel zeigt, wie Sie ein Connector-Handbuch über die alternative Quelle öffnen.

1. Melden Sie sich bei CA Support Online an.
2. Wählen Sie im Dropdown-Listenfeld "Produkt auswählen" den CA Enterprise Log Manager.
3. Blättern Sie zum Produktstatus, und wählen Sie "CA Enterprise Log Manager Certification Matrix".
4. Wählen Sie die Produktintegrationsmatrix.
5. Suchen Sie die Kategorie für die Integration, die mit der Ereignisquelle verknüpft ist, die Sie konfigurieren. Wenn es sich bei der Ereignisquelle beispielsweise um das AIX-Betriebssystem handelt, gehen Sie zur Kategorie "Betriebssystem", und klicken Sie auf die AIX-Verknüpfung.

Produkt	Version	Log-Sensor
Betriebssysteme		
AIX	5.1 5.2 5.3	syslog

Bearbeiten des Syslog-Connectors

Jeder CA Enterprise Log Manager verfügt über einen Standardagent. Wenn CA Enterprise Log Manager installiert wurde, verfügt der Standardagent über einen teilweise konfigurierten Connector mit Namen "Syslog_Connector", der auf dem Listener "Syslog" basiert. Der Listener empfängt Syslog-Rohereignisse auf den Standard-Ports, sobald Sie die Ereignisquellen konfiguriert haben, die Syslogs an CA Enterprise Log Manager senden sollen. Damit CA Enterprise Log Manager diese Rohereignisse verfeinern kann, müssen Sie diesen Syslog_Connector editieren. Bestimmte Bearbeitungen sind erforderlich, andere sind optional.

- Sie müssen die Syslog-Ziele angeben, wenn Sie diesen Connector bearbeiten. Als Syslog-Ziele wählen Sie jede Integration, die einer oder mehreren Ereignisquellen entspricht, die Sie konfiguriert haben oder konfigurieren möchten. Durch die Angabe der Syslog-Ziele ist CA Enterprise Log Manager in der Lage, Ereignisse korrekt zu verfeinern.
- Optional können Sie Unterdrückungsregeln anwenden, die Akzeptanz von Syslogs für vertrauenswürdige Hosts beschränken, neben 514 (dem bekannten UDP-Port) und 1468 (dem Standard-TCP-Port) noch weitere Ports zum Abhören festlegen und/oder eine neue Zeitzone für einen vertrauenswürdigen Host hinzufügen.

So bearbeiten Sie den Syslog-Connector für einen Standardagent:

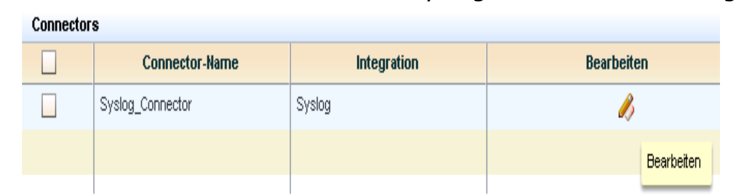
1. Klicken Sie auf die Registerkarte "Verwaltung".

   Die untergeordnete Registerkarte "Protokollerfassung" wird angezeigt.

2. Erweitern Sie den Agent-Explorer und dann die Standard-Agentengruppe oder die benutzerdefinierte Gruppe mit dem zu konfigurierenden CA Enterprise Log Manager.

3. Wählen Sie den Namen eines CA Enterprise Log Manager-Servers.

   Der Connector mit dem Namen Syslog_Connector wird angezeigt.



4. Klicken Sie auf Bearbeiten.

   Der Assistent zum Bearbeiten von Connectors wird geöffnet. Der Schritt "Connector-Details" ist ausgewählt.

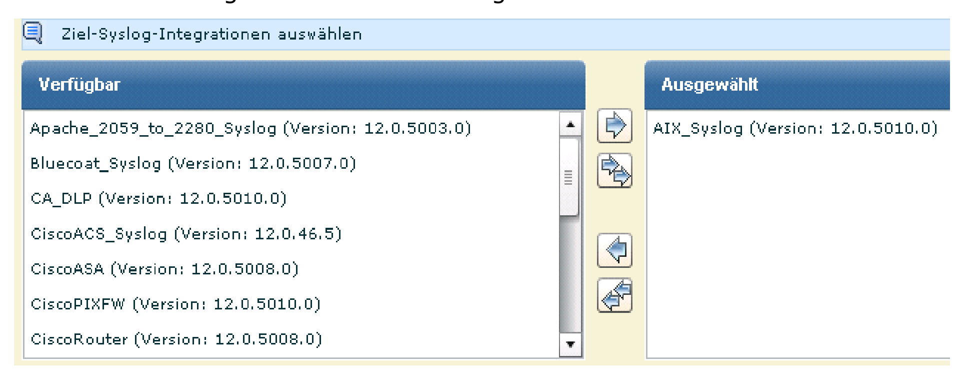
5. (Optional) Klicken Sie auf "Unterdrückungsregeln anwenden". Wenn Sie bestimmte Syslog-Ereignistypen unterdrücken, also *nicht* erfassen möchten, verschieben Sie diesen Ereignistyp von der Liste "Verfügbar" in die Liste "Ausgewählt". Wählen Sie das Ereignis, das Sie verschieben möchten, und klicken Sie auf die Schaltfläche "Verschieben".

6. Klicken Sie auf den Schritt "Connector-Konfiguration".

   Standardmäßig werden alle verfügbaren Integrationen ausgewählt.

7. Wählen Sie Syslog-Ziele, indem Sie die Syslog-Integrationen für Ziele von der Liste "Verfügbar" in die Liste "Ausgewählt" verschieben.

   Wenn Sie beispielsweise das AIX-Betriebssystem auf einem Host in Ihrem Netzwerk konfiguriert haben, sollten Sie das Syslog-Ziel "AIX_Syslog" aus der Liste "Verfügbar" in die Liste "Ausgewählt" verschieben.



8. (Optional) Geben Sie die vertrauenswürdigen Hosts an, von denen der Syslog-Connector eingehende Ereignisse akzeptieren soll. Geben Sie in das Eingabefeld die IP-Adresse ein, und klicken Sie auf "Hinzufügen". Wiederholen Sie dies für alle vertrauenswürdigen Hosts. Wenn dann ein Ereignis von einem Host empfangen wird, der nicht als vertrauenswürdig konfiguriert wurde, wird dieses Ereignis abgelehnt.

   Hinweis: Es ist eine gute Übung, vertrauenswürdige Hosts zu konfigurieren. Normalerweise konfigurieren Sie alle Hosts, auf denen Sie Ereignisse konfiguriert haben, die Syslogs an CA Enterprise Log Manager senden sollen. Durch die Angabe von vertrauenswürdigen Hosts stellen Sie sicher, dass der Standardagent keine Ereignisse von Schurkensystemen akzeptiert, die ein Angreifer konfiguriert hat, um Ereignisse an den Syslog-Listener zu senden.

9. (Optional) Fügen Sie Ports hinzu.

   Sie können typischerweise die Standard-UPD- und TCP-Ports für den Standardagent akzeptieren.

   Hinweis: Sie erreichen Leistungsverbesserungen, indem Sie einen Syslog-Connector für verschiedene Ereignistypen definieren und für jeden einen eigenen Port festlegen. Stellen Sie sicher, dass die Ports nicht verwendet werden, wenn Sie neue Ports zuweisen.

10. (Optional) Fügen Sie nur eine Zeitzone hinzu, wenn Sie Syslogs von Geräten erfassen, deren Zeitzone sich von der Soft-Appliance unterscheidet.

    a. Klicken Sie auf "Ordner erstellen", und erweitern Sie den Ordner.

    b. Markieren Sie den leeren Eintrag unter dem Ordner. Geben Sie die IP-Adresse eines vertrauenswürdigen Hosts ein, den Sie für diesen Connector definiert haben, oder den NTP-Time-Server, den Sie bei der Installation von CA Enterprise Log Manager festgelegt haben.



11. Klicken Sie auf "Speichern" und "Schließen".

12. Zeigen sie den Staus an.

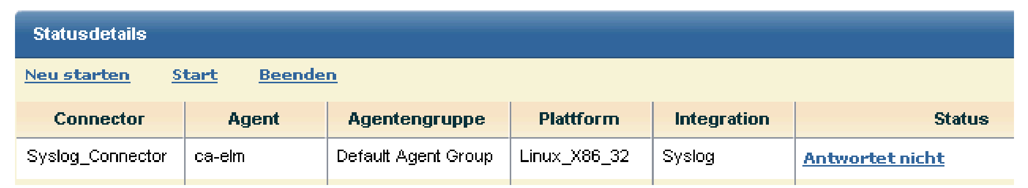
    a. Klicken Sie auf "Status und Befehl".



       "Anzeigen des Status von Agents" ist ausgewählt. In der Spalte "Agenten" wird der Hostname des installierten Servers angezeigt, da sich der Standardagent auf diesem Server befindet. Der Status "Wird ausgeführt" wird angezeigt.

    b. Klicken Sie auf den Link "Wird ausgeführt", um Details anzuzeigen.

    c. Klicken Sie auf die Schaltfläche "Connectors", um den Status des Connectors anzuzeigen.



Statusdetails

Neu starten Start Beenden

Connector	Agent	Agentengruppe	Plattform	Integration	Status
Syslog_Connector	ca-elm	Default Agent Group	Linux_X86_32	Syslog	Antwortet nicht

d. Klicken Sie auf den Link "Wird ausgeführt".

   Die Felder "Prozent der CPU", "Arbeitsspeicherverwendung", Durchschnittliche Ereignisse pro Sekunde (EPS)" und "Anzahl der gefilterten Ereignisse" werden angezeigt.

Anzeigen von Syslog-Ereignissen

Eine der schnellsten Möglichkeiten, Abfrageergebnisse für Ereignisse anzuzeigen, die von einem Syslog-Listener erfasst wurden, ist die Verwendung der Eingabeaufforderung für den Host.

So zeigen Sie Syslog-Ereignisse an:

1. Wählen Sie die Registerkarte "Abfragen und Berichte".

   Die untergeordnete Registerkarte "Abfragen" wird angezeigt.

2. Erweitern Sie die Eingabeaufforderung auf der Abfrageliste, und wählen Sie den Host.

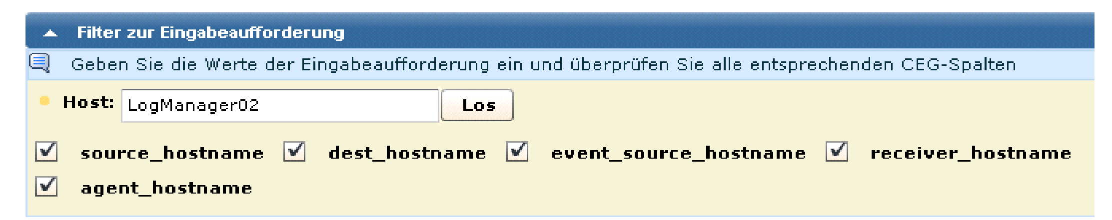


3. Übermitteln Sie eine Abfrage für Ereignisse, die vom Standardagent erfasst wurden.

   a. Geben Sie den Namen des Standardagents im Feld "Host" ein. Dies ist auch der Name des CA Enterprise Log Manager, auf dem er sich befindet.

   b. Wählen Sie "agent_hostname".

   c. Klicken Sie auf "Los".



4. Zeigen Sie die Ergebnisse an, die weiter verfolgt werden sollen.

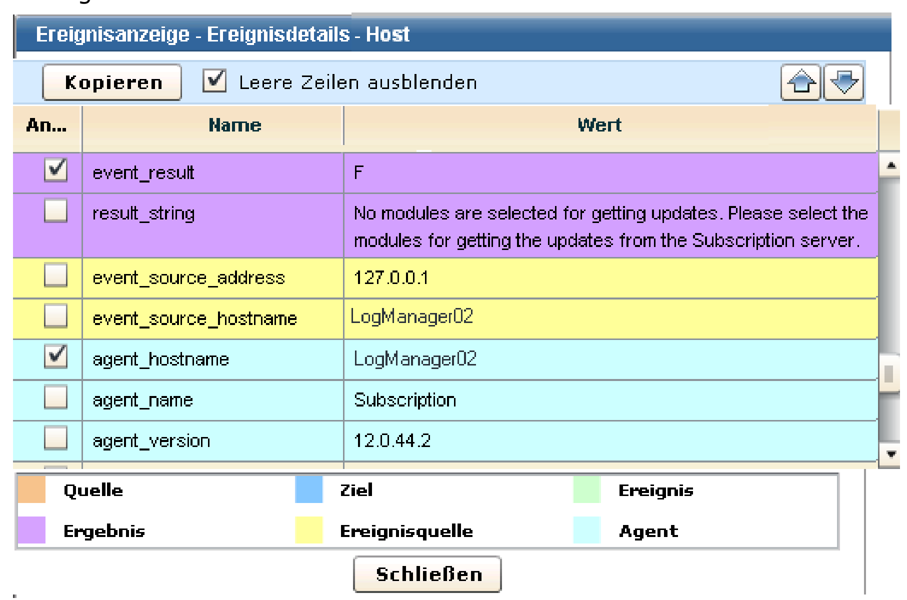
   a. Klicken Sie auf die Spalte "Ergebnisse", um nach Ergebnissen zu sortieren.

   b. Blättern Sie zum ersten Ergebnis für "F" wie "Fehler". Angenommen, es handelt sich dabei um eine Konfigurationswarnung der Kategorie "Konfigurationsverwaltung".

   c. Doppelklicken Sie auf die Zeile, um die Details anzuzeigen.

   Die Ereignisanzeige wird geöffnet.

5. Blättern Sie zu dem Bereich, in dem das Ergebnis angezeigt wird. In diesem Beispiel handelt es sich bei dem Fehler um eine Warnung, die Sie im Modul für automatische Software-Updates konfigurieren müssen. Diese Warnung sollten Sie ignorieren, bis Sie alle gewünschten CA Enterprise Log Manager-Server installiert haben.



Kapitel 3: Bereitstellung von Windows-Agents

Dieses Kapitel enthält folgende Themen:

Erstellen eines Benutzerkontos für den Agent

Bevor Sie einen Agent auf einem Windows-Betriebssystem installieren, erstellen Sie im Ordner der Windows-Benutzer ein Konto für den Agent. Ziel dieses Agentkontos mit eingeschränkten Rechten ist es, den Agent mit den geringsten Berechtigungen auszuführen. Sie geben den Benutzernamen und das Kennwort ein, die Sie hier bei der Installation des Agents erstellt haben.

Hinweis: Sie können diesen Schritt überspringen und bei der Installation die Anmeldeinformationen der Domäne eines Administrators für den Agent eingeben. Diese Vorgehensweise wird jedoch nicht empfohlen.

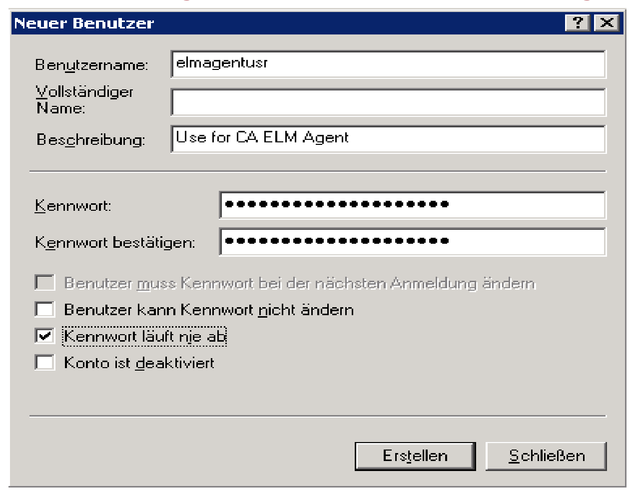
So erstellen Sie ein Windows-Benutzerkonto für den Agent:

1. Melden Sie sich bei dem Host an, auf dem Sie den Agent installieren möchten. Verwenden Sie die Verwaltungsanmeldeinformationen.
2. Klicken Sie auf "Start", "Programme", "Verwaltung", "Computerverwaltung".
3. Erweitern Sie "Lokale Benutzer und Gruppen".
4. Klicken Sie mit der rechten Maustaste auf "Benutzer" und wählen Sie "Neuer Benutzer".

   Das Windows-Dialogfeld "Neuer Benutzer" wird geöffnet.

5. Geben Sie einen Benutzernamen und das Kennwort ein. Bestätigen Sie das Kennwort durch erneute Eingabe. Ein effektives Kennwort besteht aus einer Mischung von alphanumerischen Zeichen und Sonderzeichen. Beispiel: calmr12_agent. Optional können Sie eine Beschreibung eingeben.

   Wichtig! Notieren Sie den Namen und das Kennwort oder speichern Sie sie. Sie benötigen ihn bei der Installation des Agents.



6. Klicken Sie auf "Erstellen". Klicken Sie auf "Schließen".

Weitere Informationen:

Installieren eines Agents (siehe Seite 39)

Festlegen des Authentifizierungsschlüssels für einen Agenten

Bevor Sie den ersten Agent installieren, müssen Sie den Authentifizierungsschlüssel des Agents kennen. Sie können den Standardwert verwenden, wenn kein Schlüssel festgelegt wurde, den aktuellen Schlüssel verwenden, sofern ein solcher eingerichtet wurde, oder einen neuen Schlüssel festlegen. Der hier konfigurierte Authentifizierungsschlüssel des Agenten muss bei der Installation der einzelnen Agents angegeben werden. Dieser Schritt kann nur von einem Administrator durchgeführt werden.

So legen Sie den Authentifizierungsschlüssel des Agenten fest:

1. Öffnen Sie den Browser auf dem Host, auf dem Sie den Agent installieren möchten, und geben Sie die URL des CA Enterprise Log Manager-Servers für diesen Agent an. Beispiel:

   https://<IP-Adresse>:5250/spin/calm/

2. Melden Sie sich beim CA Enterprise Log Manager-Server an. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf "Anmelden".
3. Klicken Sie auf die Registerkarte "Verwaltung".

   Im linken Fensterbereich wird der Protokollerfassungs-Explorer angezeigt.

4. Wählen Sie den Agent-Explorer-Ordner.

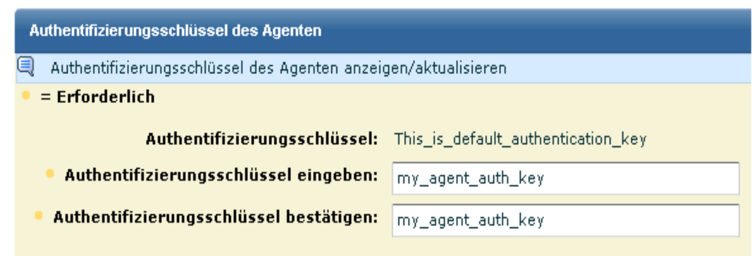
   Im Hauptbereich wird eine Symbolleiste angezeigt.

5. Klicken Sie auf "Authentifizierungsschlüssel des Agenten".

6. Geben Sie den Authentifizierungsschlüssel des Agenten ein, der für die Agentinstallation verwendet werden soll, oder notieren Sie den aktuellen Eintrag.

   Wichtig! Notieren Sie diesen Schlüssel oder zeichnen Sie ihn auf. Sie benötigen ihn bei der Installation des Agents.

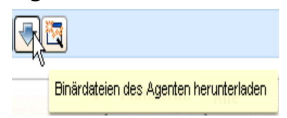
7. Klicken Sie auf "Speichern".
8. Fahren Sie mit dem Herunterladen des Agentinstallationsprogramms fort (nächster Schritt).

Herunterladen des Agentinstallationsprogramms

Wenn Sie nur den Authentifizierungsschlüssel des Agenten festlegen, können Sie das Agentinstallationsprogramm auf den Desktop herunterladen.

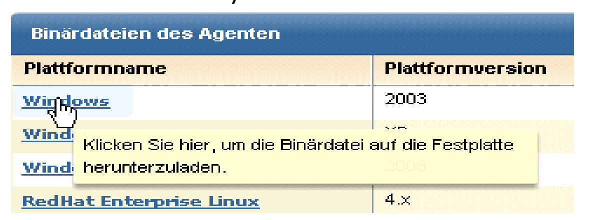
So laden Sie das Agentinstallationsprogramm herunter:

1. Klicken Sie in der Symbolleiste des Agent-Explorers auf "Binärdateien des Agents herunterladen".

   Im Hauptbereich werden Verknüpfungen zu den verfügbaren Binärdateien des Agents angezeigt.

2. Klicken Sie auf die Windows-Verknüpfung, um den Agent auf einem Server mit dem Betriebssystem Windows Server 2003 zu installieren.

   Das Dialogfeld "Speicherort für den Download nach <IP-Adresse>" wird geöffnet.

3. Wählen Sie den Desktop, und klicken Sie auf "Speichern".

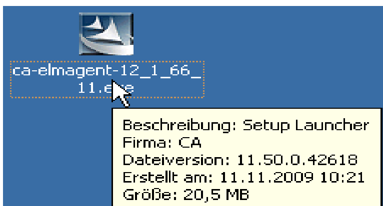
   

   Es wird ein Meldungsfeld geöffnet, das den Fortschritt des Downloads der ausgewählten Binärdateien des Agents anzeigt, gefolgt von einer Bestätigungsmeldung.

4. Klicken Sie auf "OK".

5. Minimieren Sie den Browser, unterbrechen Sie jedoch nicht die Verbindung, so dass Sie die Installation schnell überprüfen können, nachdem sie abgeschlossen ist.

   Auf dem Desktop wird das Setup-Startprogramm für die Agentinstallation angezeigt.

Installieren eines Agents

Bevor Sie beginnen, sollten Sie Folgendes bereit halten:

- IP-Adresse des CA Enterprise Log Manager-Servers, von dem Sie das Agentprogramm heruntergeladen haben
- Benutzername und Kennwort des Benutzerkontos, das Sie für den Agent erstellt haben
- Authentifizierungsschlüssel des Agenten, den Sie festgelegt haben

So installieren Sie einen Agent für einen Windows-Host:

1. Doppelklicken Sie auf das Startprogramm für die Agentinstallation.

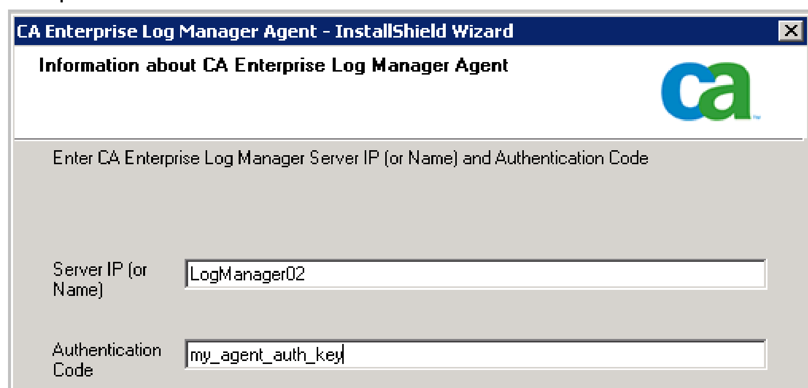
   Der Installations-Assistent wird gestartet.

2. Klicken Sie auf "Weiter", lesen Sie den Lizenzvertrag, klicken Sie auf "Ich stimme den Bedingungen des Lizenzvertrags zu.", um fortzufahren, und klicken Sie auf "Weiter".
3. Akzeptieren Sie den angebotenen Installationspfad oder ändern Sie ihn, und klicken Sie auf "Weiter".
4. Geben Sie die erforderlichen Informationen wie folgt ein:
   a. Geben Sie den Hostnamen des CA Enterprise Log Manager-Servers ein, an den dieser Agent die erfassten Protokolle weiterleiten soll.

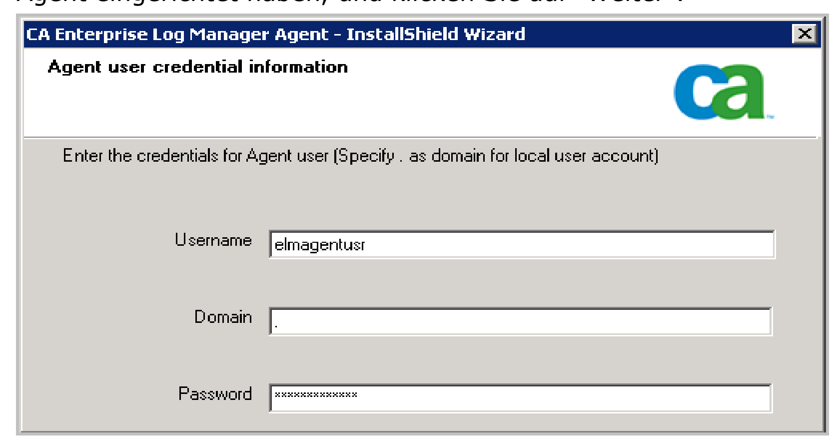
      Hinweis: Da CA Enterprise Log Manager in diesem Beispielszenario DHCP für die IP-Adressenzuordnung verwendet, dürfen Sie hier keine IP-Adresse eingeben. Andernfalls besteht die Gefahr, dass der Agent neu installiert werden muss, falls sich die IP-Adresse des Servers ändert.

b. Geben Sie den Authentifizierungsschlüssel des Agenten ein.

Beispiel:



5. Geben Sie Namen und Kennwort des Benutzerkontos ein, das Sie für den Agent eingerichtet haben, und klicken Sie auf "Weiter".



6. Klicken Sie auf "Weiter". Optional können Sie eine Datei für den exportierten Connector angeben.

   Die Seite "Kopieren der Dateien starten" wird angezeigt.

7. Klicken Sie auf "Weiter".

   Die Installation des Agents ist abgeschlossen.

8. Klicken Sie auf "Fertig stellen".

9. Fahren Sie mit der Konfiguration der Connectors für diesen Agent fort.

   Nachdem Sie die Connectors konfiguriert haben, werden die erfassten Ereignisse über Port 17001 an den CA Enterprise Log Manager-Ereignisprotokollspeicher gesendet.

   Wichtig! Wenn Sie über den Host, auf dem Sie den Agent installiert haben, keinen ausgehenden Datenverkehr zulassen und die Windows Firewall verwenden, müssen Sie diesen Port auf Ihrer Windows Firewall öffnen.

Weitere Informationen:

Herunterladen des Agentinstallationsprogramms (siehe Seite 38)
Erstellen eines Benutzerkontos für den Agent (siehe Seite 35)
Festlegen des Authentifizierungsschlüssels für einen Agenten (siehe Seite 37)

Erstellen eines Connectors basierend auf NTEventLog

Nach der Installation eines Agents können Sie einen Connector erstellen, um die Ereignisquelle für die Erfassung von Ereignissen festzulegen. Da Sie einen Agent auf einem Server mit Windows-Betriebssystem installiert haben, erstellen Sie einen Connector basierend auf der NTEventLog-Integration und legen die Einstellungen für den WMILogSensor wie im Connector-Handbuch beschrieben fest. Dieses Handbuch öffnen Sie über den Assistenten zum Erstellen neuer Connectors. Sie geben den Namen des Hosts an, auf dem der Agent für eine agentbasierte Protokollerfassung installiert ist. Optional können Sie einen anderen WMI Protokollsensor für diesen Connector hinzufügen und einen Host angeben, der nicht dem Host entspricht, auf dem der Agent installiert ist. So ermöglichen Sie die Protokollverbindung ohne Agent. Der/die zusätzliche(n) Host(s) müssen sich in derselben Domäne befinden und über denselben Windows-Administrator verfügen wie der erste hinzugefügte Host.

So erstellen Sie einen Connector basierend auf NTEventLog:

1. Maximieren Sie den Browser, der den CA Enterprise Log Manager Agent-Explorer anzeigt.
2. Erweitern Sie den Agent-Explorer und anschließend die Standard-Agentengruppe.

   Der Name des Computers, auf dem der Agent installiert wurde, wird angezeigt.

3. Wählen Sie diesen Agent.

   Das Feld "Agenten-Connectors" wird angezeigt.

4. Klicken Sie auf "Neuen Connector erstellen".

   Der Assistent zum Erstellen von neuen Connectors wird geöffnet. Der Schritt "Erstellung von neuem Connector" ist ausgewählt.

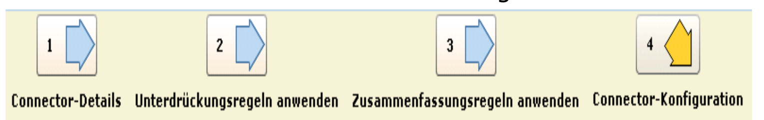
5. Belassen Sie die Auswahl von "Integrationen" und wählen Sie aus der Integrations-Dropdownliste NTEventLog.

   Die Felder "Connector-Name" und "Beschreibung" werden auf Grundlage der Auswahl unter "Integration" ausgefüllt.

6. Bearbeiten Sie den Connector-Namen, um einen eindeutigen Namen zu definieren. Erweitern Sie den Namen möglicherweise durch den Namen des Zielservers, z. B. NTEventLog_Connector_USER001LAB.



7. Wählen Sie den Schritt "Connector-Konfiguration".



   Der Bereich "Sensorkonfiguration" wird eingeblendet. Er enthält eine Hilfe-Schaltfläche mit einer Verknüpfung zum Connector-Handbuch für NTEventLog, in dem Sie Hilfe zu den Feldern für die Sensorkonfiguration finden.

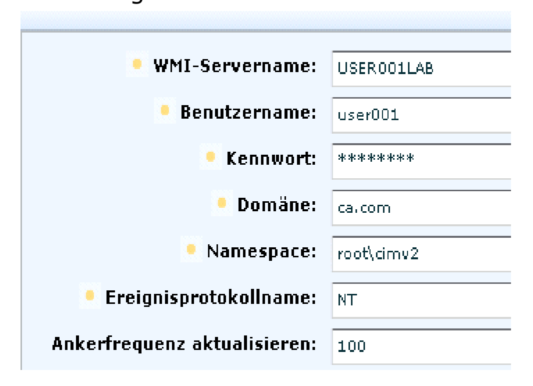


8. Klicken Sie auf die Schaltfläche zum Anzeigen von Details für WMI-Quellen.

Connector-Konfiguration
Geben Sie die Konfigurationsdetails ein
Gespeicherte Konfigurationen: Konfiguration auswählen
Sensorkonfiguration
WMI-Quellen:
Details anzeigen

9. Konfigurieren Sie die WMILogSensor-Einstellungen des lokalen Computers für die agentbasierte Protokollerfassung. Weitere Informationen erhalten Sie, wenn Sie auf "Hilfe" klicken.

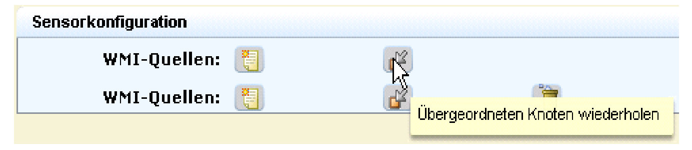
   Das folgende Beispiel zeigt eine Konfiguration, bei der der Benutzer ein Windows-Administrator auf dem angegebenen WMI-Server ist. Die Domäne gilt für den WMI-Server.



10. (Optional) Konfigurieren Sie mit demselben Connector einen WMI-Sensor für einen anderen Computer für die Protokollerfassung ohne Agent.

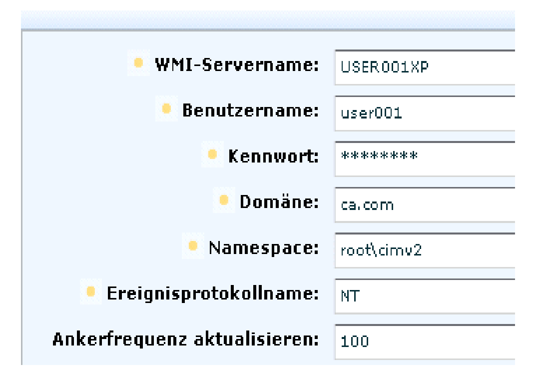
    a. Klicken Sie auf die Schaltfläche "Übergeordneten Knoten wiederholen".

       Die folgende Abbildung zeigt eine Konfiguration mit zwei WMI-Quellen.



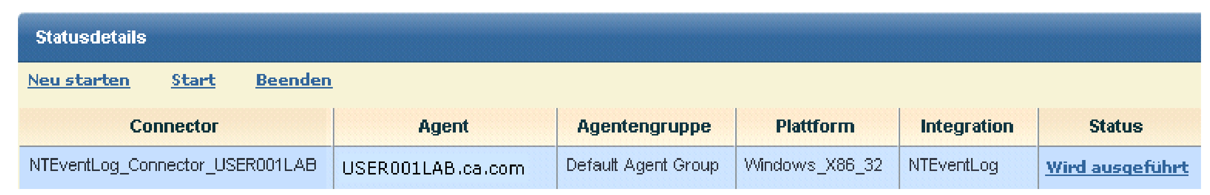
b. Konfigurieren Sie die WMILogSensor-Einstellungen für einen anderen Computer.

Das folgende Beispiel zeigt eine Konfiguration für einen zweiten WMI-Protokollsensor in derselben Domäne und mit denselben Administrator-Anmeldeinformationen.



11. Klicken Sie auf "Speichern" und "Schließen".
12. Um den Status des Connectors anzuzeigen, den Sie konfiguriert haben, gehen Sie folgendermaßen vor:
    a. Wählen Sie im linken Fensterbereich den Agent aus.
    b. Klicken Sie auf "Status und Befehl".
    c. Wählen Sie "Anzeigen des Status von Connectors".

    Das Fenster "Statusdetails" wird angezeigt.



Statusdetails

Neu starten Start Beenden

Connector	Agent	Agentengruppe	Plattform	Integration	Status
NTEventLog_Connector_USER001LAB	USER001LAB.ca.com	Default Agent Group	Windows_X86_32	NTEventLog	Wird ausgeführt

13. Klicken Sie auf den Link "Wird ausgeführt".

    Der angezeigte Status des Ziels, das im Connector konfiguriert wurde, umfasst Prozent der CPU, Arbeitsspeicherverwendung und durchschnittliche Ereignisse pro Sekunde (EPS).

Konfigurieren einer Windows-Ereignisquelle

Nachdem Sie einen Connector mit der NTEventLog-Integration auf dem Agent konfiguriert haben, sollten Sie Ereignisse in der Ereignisanzeige anzeigen können. Falls Ereignisse nicht an die Ereignisanzeige weitergeleitet werden, sollten Sie die Windows-Einstellungen für die lokalen Richtlinien auf der Ereignisquelle ändern.

So konfigurieren Sie lokale Richtlinien auf der Ereignisquelle für einen NTEventLog-Connector:

1. Wenn der Protokollerfassungs-Explorer nicht bereits angezeigt wird, klicken Sie auf die Registerkarte "Verwaltung".
2. Erweitern Sie die Punkte "Ereignisverfeinerungs-Bibliothek", "Integrationen" und "Automatische Software-Updates", wählen Sie "NTEventLog", und klicken Sie auf die Hilfeverknüpfung über dem Integrationsnamen im Teilfenster "Integrationsdetails anzeigen".

   Das Connector-Handbuch für das NT-Ereignisprotokoll (Sicherheit, Anwendung, System) wird geöffnet.

3. Minimieren Sie die Benutzeroberfläche von CA Enterprise Log Manager, und befolgen Sie die Anweisungen im Connector-Handbuch, um lokale Richtlinien einer Ereignisquelle auf einem Windows-Betriebssystem zu bearbeiten.

   Hinweis: Wenn es sich bei Ihrem System um Windows Server 2003 handelt, wählen Sie in der Systemsteuerung die Optionen "Verwaltung", "Lokale Sicherheitsrichtlinie", und erweitern Sie anschließend die lokalen Sicherheitsrichtlinien.

4. (Optional) Wenn Sie einen WMI-Sensor für einen zweiten WMI-Server konfiguriert haben, bearbeiten Sie auch die lokalen Richtlinien dieses Servers.
5. Maximieren Sie CA Enterprise Log Manager.

Anzeigen von Protokollen der Windows-Ereignisquellen

Eine der schnellsten Möglichkeiten, Abfrageergebnisse für eingehende Ereignisse anzuzeigen, ist die Verwendung der Eingabeaufforderung für den Host. Sie können auch Abfragen oder Berichte auswählen.

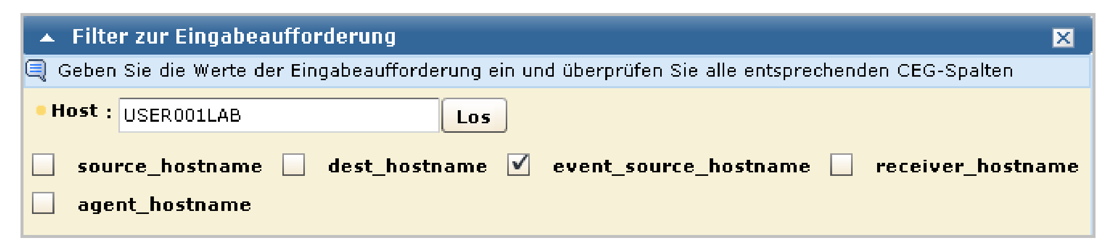
So zeigen Sie eingehende Ereignisprotokolle an:

1. Wählen Sie die Registerkarte "Abfragen und Berichte".

   Die untergeordnete Registerkarte "Abfragen" wird angezeigt.

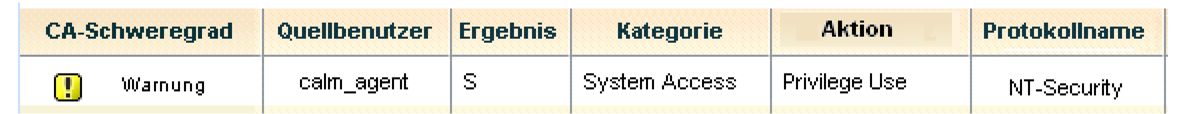
2. Erweitern Sie die Eingabeaufforderung auf der Abfrageliste, und wählen Sie den Host.

3. Geben Sie den Namen des WMI-Servers ein, der im Feld "Host" für den Sensor konfiguriert wurde. Entfernen Sie alle anderen Markierungen, und klicken Sie auf "Los".



Die Ereignisse der WMI-Server-Ereignisquelle werden angezeigt.

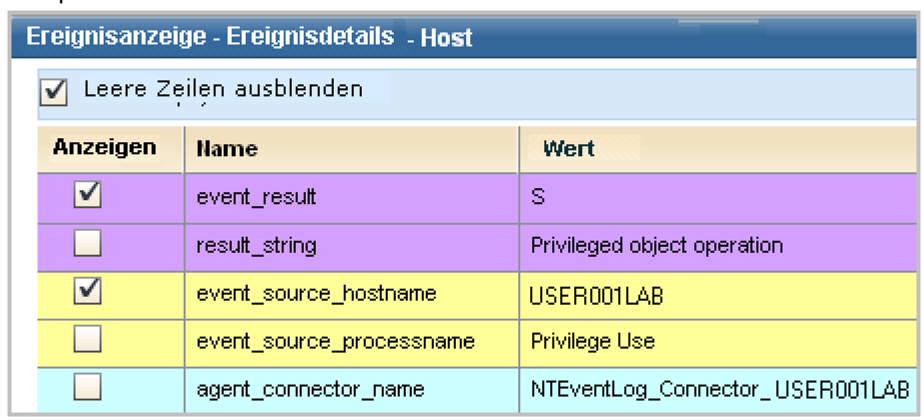
4. Klicken Sie auf "CA-Schweregrad", und blättern Sie, bis Sie eine Warnung gefunden haben. Im Folgenden wird ein verkürztes Beispiel ohne die Spalten "Datum" und "Ereignisquelle" angezeigt:



CA-Schweregrad	Quellbenutzer	Ergebnis	Kategorie	Aktion	Protokollname
Warnung	calm_agent	S	System Access	Privilege Use	NT-Security

5. Klicken Sie auf "Rohereignisse anzeigen", um die Rohereignisse für die Warnung anzuzeigen.

6. Doppelklicken Sie auf die Warnung, um die Ereignisanzeige mit weiteren Daten zu öffnen. Das folgende Beispiel zeigt einige Zeilen mit Beispieldaten:

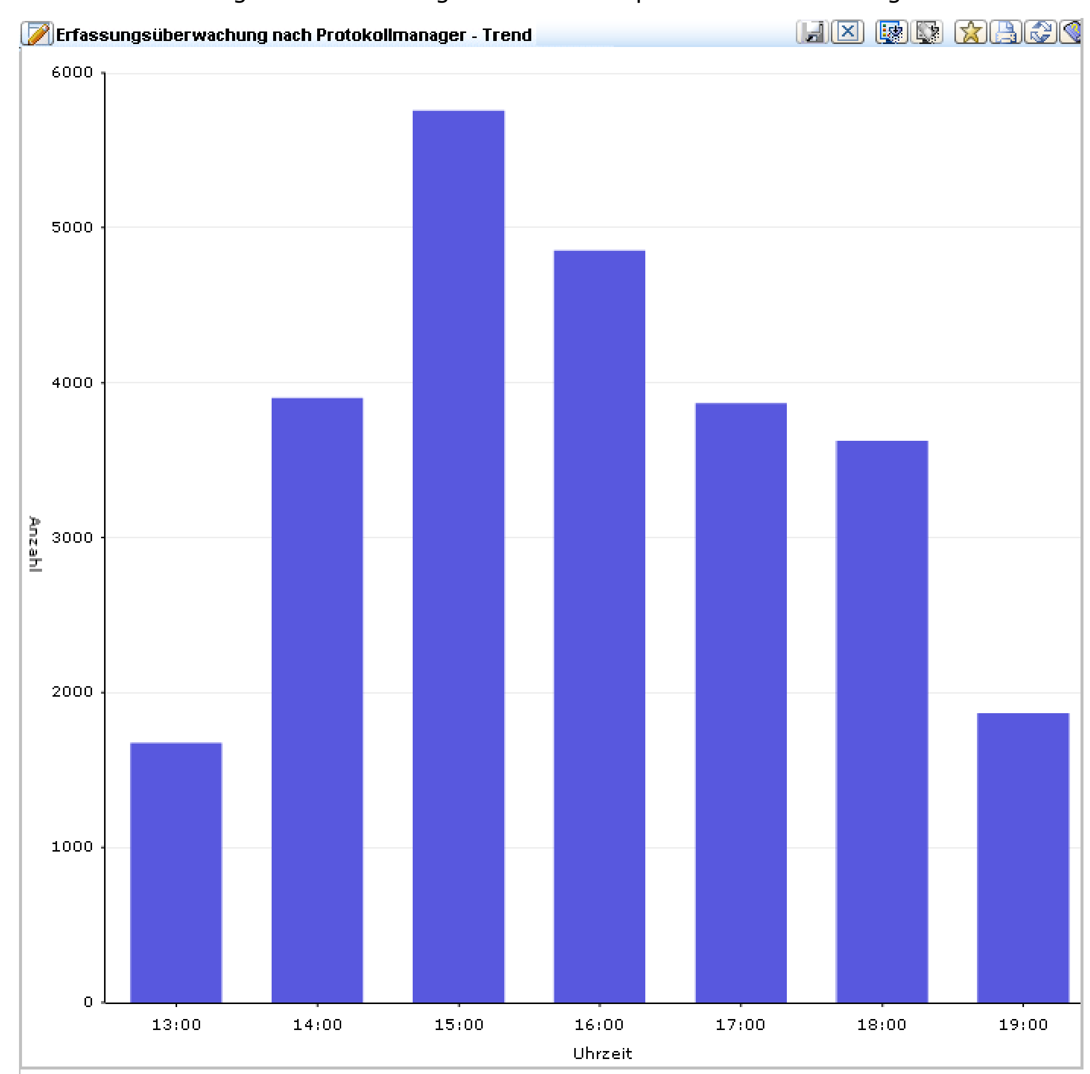


Ereignisanzeige - Ereignisdetails - Host

Leere Zeilen ausblenden

Anzeigen	Name	Wert
☑	event_result	S
☐	result_string	Privileged object operation
☑	event_source_hostname	USER001LAB
☐	event_source_processname	Privilege Use
☐	agent_connector_name	NTEventLog_Connector_USER001LAB

7. Klicken Sie auf die Registerkarte "Abfragen und Berichte", klicken Sie in der Abfrageliste auf eine Abfrage, z. B. "Erfassungsüberwachung nach Log Manager - Trend". Zeigen Sie das entsprechende Balkendiagramm an.



8. Klicken Sie auf "Berichte". Geben Sie unter "Berichtsliste" im Feld "Suchen" den Eintrag "selbst" ein, um den Berichtsnamen "Selbstüberwachende Ereignisse des Systems" anzuzeigen. Wählen Sie diesen Bericht, um eine Liste der Ereignisse anzuzeigen, die vom CA Enterprise Log Manager-Server generiert wurden.

Hinweis: Weitere Informationen zum Planen von Berichten mit Informationen, die Sie analysieren möchten, finden Sie in der Online-Hilfe oder im *Verwaltungshandbuch*.

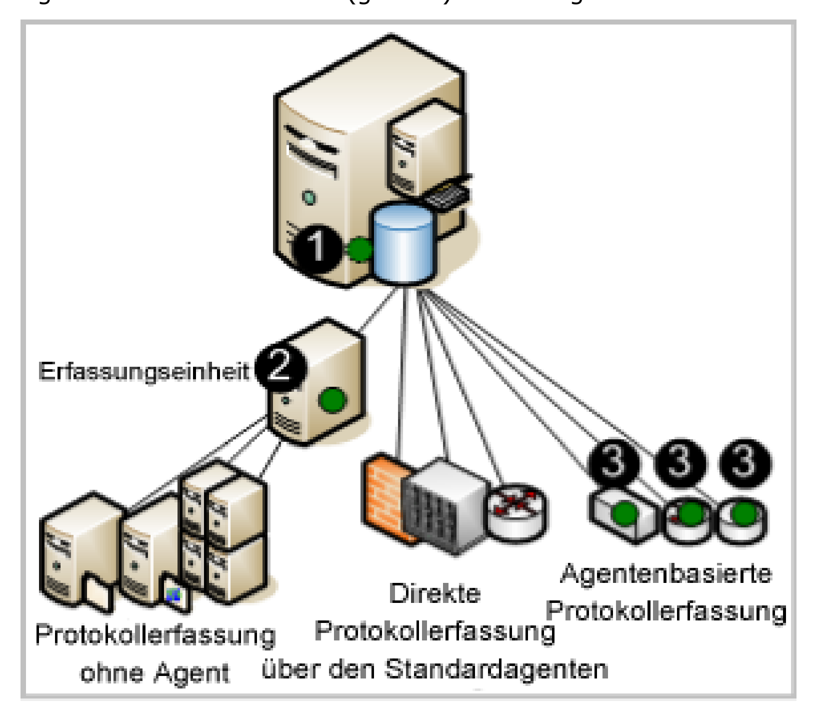
Kapitel 4: Hauptfunktionen

Dieses Kapitel enthält folgende Themen:

Protokollerfassung

Der CA Enterprise Log Manager-Server kann so eingerichtet werden, dass er Protokolle mit einer oder mehreren unterstützten Techniken erfasst. Die Techniken unterscheiden sich durch Typ und Speicherort der Komponente, die die Protokolle abhört und erfasst. Diese Komponenten werden auf Agents konfiguriert.

Die folgende Abbildung zeigt ein Single-Server-System, auf dem der Ort der Agents mit einem dunklen (grünen) Kreis dargestellt wird.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Konfigurieren Sie den Standardagent auf CA Enterprise Log Manager, um Ereignisse direkt von den angegebenen Syslog-Quellen abzurufen.
2. Konfigurieren Sie den Agent, der auf einem Windows-Sammelpunkt installiert wurde, um Ereignisse von angegebenen Windows-Servern zu erfassen und an CA Enterprise Log Manager zu senden.
3. Konfigurieren Sie Agents, die auf Hosts installiert wurden, auf denen Ereignisquellen ausgeführt werden, um den konfigurierten Ereignistyp zu erfassen und eine Unterdrückung durchzuführen.

Hinweis: Datenverkehr vom Agent zum Ziel-CA Enterprise Log Manager-Server wird immer verschlüsselt.

Die einzelnen Protokollerfassungstechniken haben folgende Vorteile:

- Direkte Protokollerfassung

  Bei der direkten Protokollerfassung konfigurieren Sie den Syslog-Listener auf dem Standardagent, so dass dieser Ereignisse von den von Ihnen angegebenen vertrauenswürdigen Quellen empfängt. Sie können andere Connectors auch so konfigurieren, dass sie Ereignisse von allen Ereignisquellen erfassen, die mit der Soft-Appliance-Plattform kompatibel sind.

  Vorteil: Sie müssen keinen Agents installieren, um Protokolle von Ereignisquellen zu erfassen, die sich in unmittelbarer Nähe des CA Enterprise Log Manager-Servers befinden.

- Erfassung ohne Agent

  Bei der Erfassung ohne Agent gibt es keinen lokalen Agent an den Ereignisquellen. Stattdessen wird an einem bestimmten Sammelpunkt ein Agent installiert. Für jede Zielereignisquelle wird auf diesem Agent ein Connector konfiguriert.

  Vorteil: Sie können Protokolle von Ereignisquellen erfassen, die auf Servern ausgeführt werden, auf denen keine Agenten installiert werden können, beispielsweise auf Servern, auf denen die Installation von Agenten aufgrund von betriebsinternen Richtlinien nicht zugelassen ist. Die Übermittlung ist garantiert, wenn beispielsweise die ODBC-Protokollerfassung korrekt konfiguriert wurde.

- Agentbasierte Erfassung

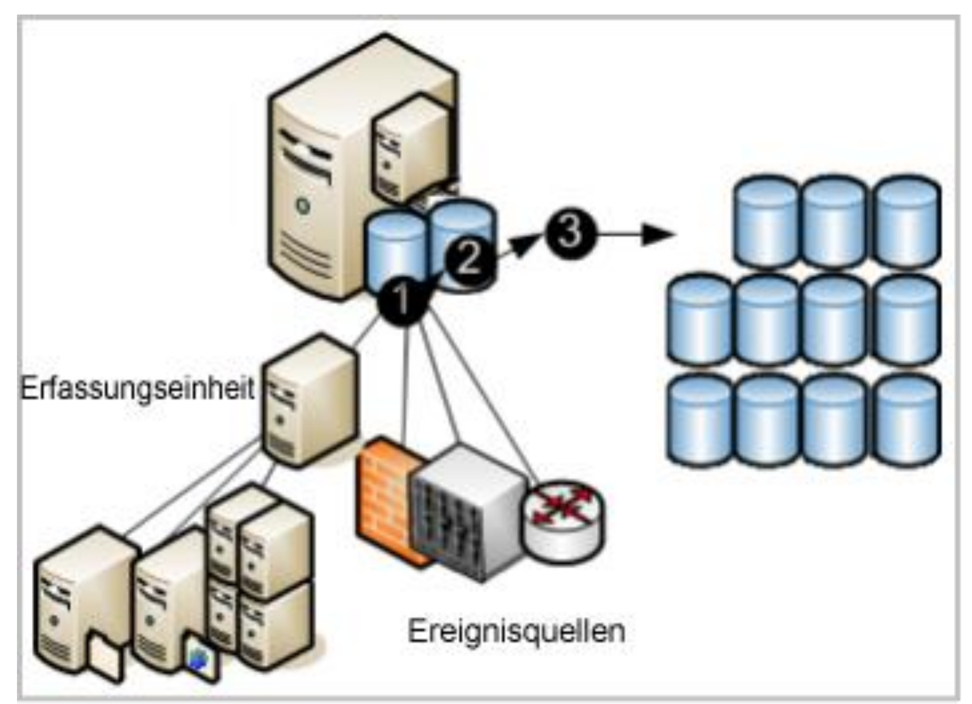
  Bei der agentbasierten Erfassung wird ein Agent überall dort installiert, wo ein oder mehrere Ereignisquellen ausgeführt werden und ein Connector für jede Ereignisquelle konfiguriert wurde.

  > Vorteil: Sie können Protokolle von Quellen erfassen, auch wenn die Bandbreite zwischen Quelle und CA Enterprise Log Manager nicht ausreicht, um eine direkte Protokollerfassung zu unterstützen. Sie können mit dem Agenten die Ereignisse filtern und so den Datenverkehr im Netzwerk reduzieren. Die Ereignisübermittlung ist garantiert.

Hinweis: Weitere Informationen zur Konfiguration von Agents finden Sie im *Verwaltungshandbuch*.

Protokollspeicherung

CA Enterprise Log Manager bietet die Möglichkeit der verwalteten eingebetteten Protokollspeicherung für kürzlich archivierte Datenbanken. Ereignisse, die durch Agenten von Ereignisquellen erfasst worden sind, durchlaufen den im folgenden Diagramm dargestellten Speicherlebenszyklus.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Neue Ereignisse werden unabhängig von der verwendeten Technik an CA Enterprise Log Manager gesendet. Der Status der eingehenden Ereignisse hängt von der verwendeten Erfassungstechnik ab. Eingehende Ereignisse müssen verfeinert werden, bevor sie in die Datenbank eingefügt werden können.
2. Wenn die Datenbank mit den verfeinerten Datensätzen die konfigurierte Größe erreicht hat, werden alle Datensätze in einer Datenbank komprimiert und unter einem eindeutigen Namen gespeichert. Durch das Komprimieren der Protokolldaten werden die Kosten für das Verschieben und Speichern der Daten reduziert. Die komprimierte Datenbank kann entweder basierend auf einer Auto-Archivierungskonfiguration automatisch verschoben werden, oder sie kann manuell gesichert und verschoben werden, bevor sie das konfigurierte Löschalter erreicht. (Automatisch archivierte Datenbanken werden sofort nach dem Verschieben aus der Quelle gelöscht.)
3. Wenn Sie komprimierte Datenbanken täglich per Auto-Archivierung auf einen Remote-Server verschieben, können Sie diese Sicherungen, falls gewünscht, in einen langfristigen Off-Site-Protokollspeicher verschieben. Mit Hilfe von beibehaltenen Protokollsicherungen können Sie die Konformität mit Gesetzen und Bestimmungen aufrechterhalten, die besagen, dass Protokolle sicher erfasst, über eine bestimmte Anzahl von Jahren zentral gespeichert und für Überprüfungen verfügbar gemacht werden müssen. (Sie können Protokolle aus einem langfristigen Speicher jederzeit wiederherstellen.)

Hinweis: Weitere Informationen zum Konfigurieren des Ereignisprotokollspeichers einschließlich der Einrichtung der Auto-Archivierung finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Wiederherstellen der Sicherungen für Untersuchungen und Berichte finden Sie im *Verwaltungshandbuch*.

Standarddarstellung von Protokollen

Protokolle, die von Anwendungen, Betriebssystemen und Geräten erstellt werden, verwenden eigene Formate. CA Enterprise Log Manager verfeinert die erfassten Protokolle, um die Datenberichte zu standardisieren. Dieses Standardformat erleichtert Auditoren und leitenden Managern den Vergleich von Daten, die in verschiedenen Quellen erfasst wurden. Technisch vereinfacht die ELM-Schemadefinition (Common Event Grammar, CEG) von CA die Implementierung der Ereignisnormalisierung und -klassifizierung.

Die ELM-Schemadefinition verwendet für die Normalisierung unterschiedlicher Ereignisaspekte verschiedene Felder. Dazu zählen folgende Felder:

- Idealmodell (Technologieklasse, z. B. Antivirus, DBMS und Firewall)
- Kategorie (z. B. Identitätsverwaltung und Netzwerksicherheit)
- Klasse (z. B. Kontenverwaltung und Gruppenverwaltung)
- Aktion (z. B. Kontenerstellung und Gruppenerstellung)
- Ergebnisse (z. B. Erfolgreich und Fehler)

Hinweis: Weitere Informationen zu den Regeln und Dateien für die Ereignisverfeinerung finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*. Details zum Normalisieren und Kategorisieren von Ereignissen finden Sie in der Online-Hilfe im Abschnitt zur ELM-Schemadefinition.

Konformitätsberichte

Mit CA Enterprise Log Manager können Sie sicherheitsrelevante Daten erfassen und verarbeiten und in Berichte für interne oder externe Auditoren umwandeln. Sie können mit Fragen und Berichten für Untersuchungen interagieren. Sie können die Berichterstellung durch die Planung von Berichtsaufträgen automatisieren.

Das System stellt Folgendes zur Verfügung:

- Leicht zu verwendende Abfragefunktion mit Kennungen
- Echtzeitnahe Berichte
- Zentral durchsuchbare, verteilte Archive kritischer Protokolle

Der Fokus liegt auf Konformitätsberichten und weniger auf der Echtzeitzuordnung von Ereignissen und Alarmen. Gesetze und Bestimmungen erfordern Berichte, mit denen die Einhaltung von branchenspezifischen Regelungen nachgewiesen werden kann. CA Enterprise Log Manager bietet Berichte mit folgenden Kennungen für eine einfache Identifizierung:

- Basel II
- COBIT
- COSO
- EU-Datenschutzrichtlinie
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Sie können vordefinierte Protokollberichte überprüfen oder auf Grundlage von selbst definierten Kriterien Suchläufe durchführen. Neue Berichte erhalten Sie mit den automatischen Software-Updates.

Protokollanzeigefunktionen werden wie folgt unterstützt:

- Bedarfsbasierte Abfragefunktion mit vordefinierten oder benutzerdefinierten Abfragen, deren Ergebnisse bis zu 5000 Datensätze umfassen können
- Schnelle Suche über Eingabeaufforderungen nach bestimmten Hostnamen, IP-Adressen, Portnummern oder Benutzernamen
- Geplante und bedarfsbasierte Berichterstattung mit standardisiertem Berichtsinhalt
- Geplante Abfragen und Alarme
- Basisberichte mit Trendinformationen
- Interaktive grafische Ereignisanzeige
- Automatische Berichterstattung mit E-Mail-Anhang
- Richtlinien zur automatischen Berichtsaufbewahrung

Hinweis: Weitere Informationen zu vordefinierten Abfragen und Berichten oder zur eigenen Erstellung finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*.

Alarm bei Verletzung von Richtlinien

Mit CA Enterprise Log Manager können Sie bei Ereignissen, die ein zeitnahes Eingreifen erfordern, das Versenden von Alarmen automatisieren. Sie können Aktionsalarme auch jederzeit über CA Enterprise Log Manager überwachen, indem Sie ein Intervall festlegen, das einen beliebigen Zeitraum von "die letzten fünf Minuten" bis "die letzten dreißig Tage" umfassen kann. Alarme werden auch automatisch an ein RSS-Feed gesendet, auf das über einen Webbrowser zugegriffen werden kann. Optional können Sie auch andere Ziele angeben, u. a. E-Mail-Adressen, einen CA IT PAM-Prozess, der beispielsweise Help-Desk-Tickets erstellt, oder eine oder mehrere SNMP-Trap-IP-Zieladressen.

Um Ihnen den Einstieg zu erleichtern, sind verschiedene vordefinierte Abfragen für die Planung von Aktionsalarmen verfügbar. Beispiele:

- Übermäßige Benutzeraktivität
- Hohe durchschnittliche CPU-Auslastung
- Geringer freier Speicherplatz
- Sicherheitsereignisprotokoll in den letzten 24 Stunden gelöscht
- Windows-Überwachungsrichtlinie in den letzten 24 Stunden geändert

Einige Abfragen verwenden Schlüssellisten, bei denen Sie die in der Abfrage verwendeten Werte verfügbar machen. Einige Schlüssellisten umfassen vordefinierte Werte, die Sie ergänzen können. Dazu gehören beispielsweise Standardkonten und berechtigte Gruppen. Andere Schlüssellisten, beispielsweise die Liste für unternehmenskritische Ressourcen, verwenden keine Standardwerte. Nach deren Konfiguration können Warnungen für vordefinierte Abfragen geplant werden, z. B.:

- Hinzufügen oder Entfernen von Gruppenmitgliedern durch berechtigte Gruppen
- Erfolgreiche Anmeldung durch Standardkonto
- Keine Ereignisse von unternehmenskritischen Quellen erhalten

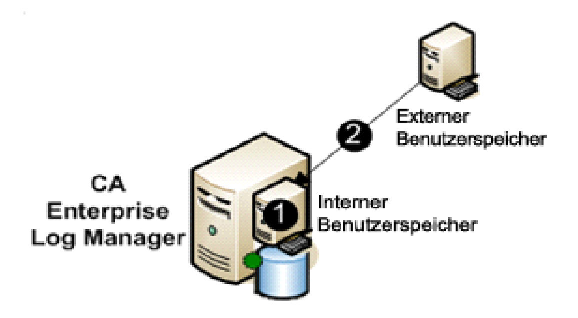
Schlüssellisten können manuell, durch Import einer Datei oder durch Ausführen eines CA IT PAM-Prozesses mit dynamischen Werten aktualisiert werden.

Hinweis: Einzelheiten zu Aktionsalarmen finden Sie im *CA Enterprise Log Manager-Administrationshandbuch*.

Verwaltung von Berechtigungen

Wenn Sie den Benutzerspeicher konfigurieren, können Sie entscheiden, ob Sie den Standardbenutzerspeicher von CA Enterprise Log Manager verwenden möchten, um Benutzerkonten einzurichten, oder ob Sie einen externen Benutzerspeicher referenzieren möchten, auf dem bereits Benutzerkonten definiert wurden. Die zugrunde liegende Datenbank ist für CA Enterprise Log Manager exklusiv. Es wird kein kommerzielles Datenbankmanagementsystem (DBMS) verwendet.

Als externe Benutzerspeicher werden CA SiteMinder und LDAP-Verzeichnisse wie beispielsweise Microsoft Active Directory, Sun One und Novell eDirectory unterstützt. Wenn Sie einen externen Benutzerspeicher referenzieren, werden die Informationen der Benutzerkonten automatisch im schreibgeschützten Format geladen (siehe Pfeil in der folgenden Abbildung). Sie definieren ausschließlich anwendungsspezifische Details für ausgewählte Konten. Es werden keine Daten vom internen Benutzerspeicher in den referenzierten externen Benutzerspeicher verschoben.



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Der interne Benutzerspeicher verwaltet Berechtigungen, indem die von den Benutzern bei der Anmeldung eingegebenen Informationen authentifiziert werden. Anschließend erhalten die Benutzer Zugriff auf verschiedene Funktionen der Benutzeroberfläche, und zwar auf der Grundlage von Berechtigungen, die mit den Rollen der entsprechenden Benutzerkonten verknüpft sind. Wenn Name und Kennwort des Benutzers, der sich anmeldet, von einem externen Benutzerspeicher geladen wurden, müssen die eingegebenen Anmeldeinformationen den geladenen Anmeldeinformationen entsprechen.
2. Der externe Benutzerspeicher dient lediglich dem Laden der Benutzerkonten in den internen Benutzerspeicher. Diese werden automatisch geladen, wenn die Referenz auf den Benutzerspeicher gespeichert wird.

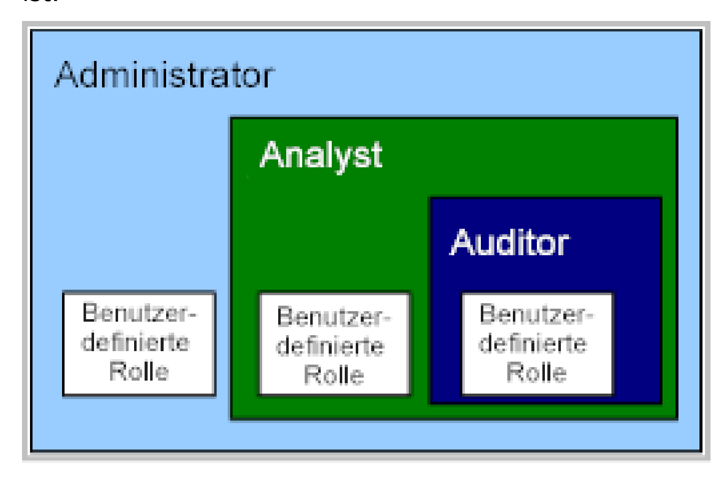
Hinweis: Weitere Informationen zum Konfigurieren des grundlegenden Benutzerzugriffs finden Sie im *Implementierungshandbuch von CA Enterprise Log Manager*. Weitere Informationen zu Richtlinien, die vordefinierte Rollen, das Erstellen von Benutzerkonten und das Zuweisen von Rollen unterstützen, finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*.

Rollenbasierter Zugriff

CA Enterprise Log Manager bietet drei vordefinierte Anwendungsgruppen oder Rollen. Administratoren weisen Benutzern folgende Rollen zu, um Zugriffsrechte für CA Enterprise Log Manager-Funktionen zu definieren:

- Administrator
- Analyst
- Auditor

Der Auditor hat Zugriff auf alle Funktionen. Der Analyst hat über die Auditor-Funktionen hinaus Zugriff auf weitere Funktionen. Der Administrator hat Zugriff auf alle Funktionen. Sie können benutzerdefinierte Rollen mit entsprechenden Richtlinien erstellen, die den Benutzerzugriff auf Ressourcen so einschränken, wie es für Ihre betriebsinternen Anforderungen erforderlich ist.



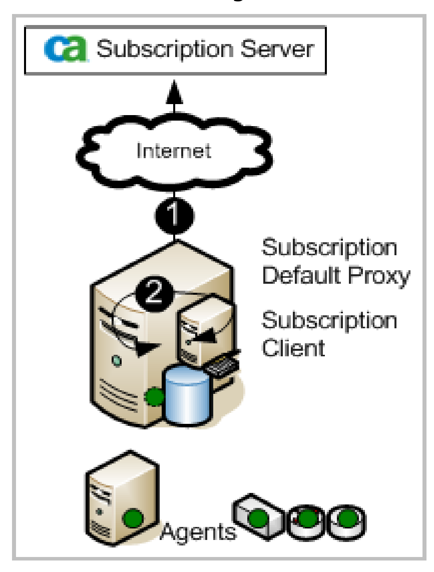
Administratoren können den Zugriff auf jede Ressource anpassen, indem sie eine benutzerdefinierte Anwendungsgruppe mit entsprechenden Richtlinien erstellen und diese Anwendungsgruppe oder Rolle bestimmten Benutzerkonten zuweisen.

Hinweis: Weitere Informationen zur Planung oder Erstellung von Rollen, benutzerdefinierten Richtlinien und Zugriffsfiltern finden Sie im *CA Enterprise Log Manager-Verwaltungshandbuch*.

Verwalten von automatischen Software-Updates

Das Modul für automatische Software-Updates ist ein Dienst, bei dem Sie automatische Software-Updates über den CA-Software-Update-Server nach einem festgelegten Plan automatisch herunterladen und an CA Enterprise Log Manager-Server verteilen können. Wenn ein automatisches Software-Update auch das Modul für Agents betrifft, wird die Bereitstellung dieser Updates an Agents durch die Benutzer initiiert. *Automatische Software-Updates* sind Aktualisierungen für CA Enterprise Log Manager-Softwarekomponenten und das Betriebssystem, Patches sowie Inhaltsaktualisierungen, wie z. B. Berichte.

Die folgende Abbildung zeigt ein Szenario mit der einfachsten direkten Internetverbindung:



Die Nummern in den Abbildungen beziehen sich auf folgende Schritte:

1. Der CA Enterprise Log Manager-Server kontaktiert als Standardserver für das Software-Update den CA-Software-Update-Server und lädt alle verfügbaren neuen Updates herunter. Der CA Enterprise Log Manager-Server erstellt eine Sicherung und verschiebt dann die Inhaltsaktualisierungen zur eingebetteten Komponente des Verwaltungsservers, der die Inhaltsaktualisierungen für alle anderen CA Enterprise Log Managers speichert.
2. Der CA Enterprise Log Manager-Server installiert als Client für automatische Software-Updates das Produkt und die benötigten Betriebssystem-Updates selbständig.

Hinweis: Weitere Informationen zum Planen und Konfigurieren von automatischen Software-Updates finden Sie im *Implementierungshandbuch*. Weitere Informationen zum Verfeinern und Bearbeiten der Konfiguration für automatische Software-Updates und für das Anwenden von Updates auf Agenten finden Sie im *Verwaltungshandbuch*.

Vorgefertigter Inhalt

CA Enterprise Log Manager umfasst vordefinierten Inhalt, den Sie verwenden können, sobald Sie das Produkt installiert und konfiguriert haben. Durch das automatische Software-Update werden regelmäßig neue Inhalte hinzugefügt und vorhandene Inhalte aktualisiert.

Kategorien vordefinierter Inhalte sind z. B.:

- Berichte mit Kennungen
- Abfragen mit Kennungen
- Integrationen mit zugehörigen Sensoren, Analysedateien (XMP), Zuordnungsdateien (DM) und, in einigen Fällen, Unterdrückungsregeln
- Unterdrückungs- und Zusammenfassungsregeln

Kapitel 5: Weitere Informationen zu CA Enterprise Log Manager

Dieses Kapitel enthält folgende Themen:

Anzeigen von Kurzinfos

Sie können die Bedeutung von Schaltflächen, Kontrollkästchen und Berichten auf der CA Enterprise Log Manager-Seite in Ihrer aktuellen Ansicht abfragen.

So zeigen Sie Kurzinfos und andere Hilfselemente an:

1. Halten Sie den Cursor über die Schaltfläche, um eine Beschreibung der entsprechenden Funktion anzuzeigen. Auf diese Weise können Sie die Funktion aller Schaltflächen anzeigen.



2. Beachten Sie den Unterschied zwischen aktiven und inaktiven Schaltflächen.

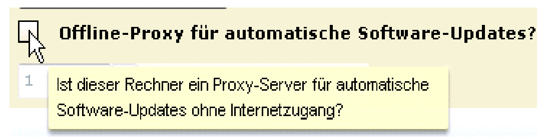
   Aktivierte Schaltflächen werden farbig angezeigt. So wird die Schaltfläche "Zugriffsfilterliste" für Administratoren der Benutzer- und Zugriffsverwaltung farbig angezeigt.



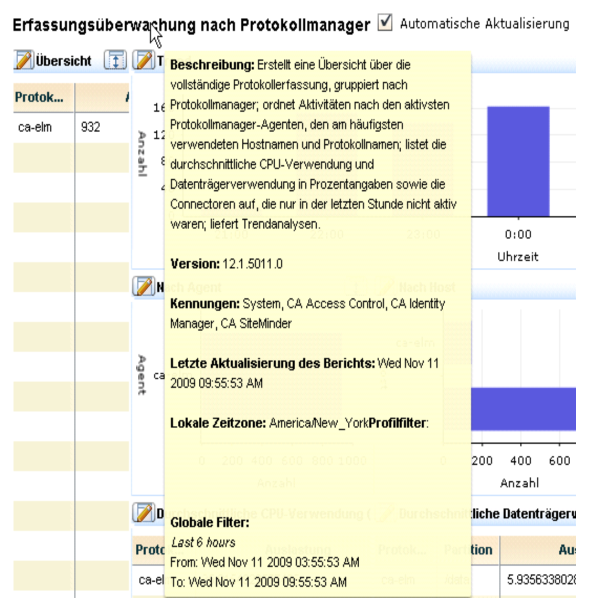
   Deaktivierte Schaltflächen werden schwarz-weiß dargestellt. So wird die Schaltfläche "Zugriffsfilterliste" für Auditoren schwarz-weiß dargestellt.



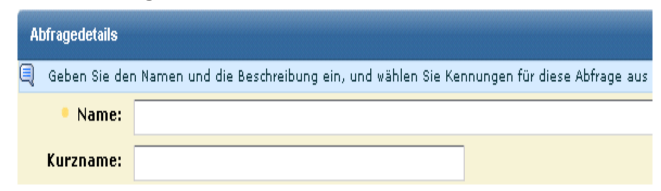
3. Zeigen Sie die Beschreibungen für Eingabefelder und Kontrollkästchen an, indem Sie den Cursor über den Feldnamen halten.



4. Zeigen Sie Beschreibungen für Berichte an, indem Sie den Cursor über den Berichtnamen halten.



5. Links neben einigen Feldern wird ein orangefarbener Punkt angezeigt. Felder mit diesem Punkt müssen ausgefüllt werden. Eine zu speichernde Konfiguration kann erst gespeichert werden, wenn alle erforderlichen Felder ausgefüllt wurden.



Anzeigen der Online-Hilfe

Sie können für die angezeigte Seite oder für jede Aufgabe, die Sie durchführen möchten, Hilfe aufrufen.

So öffnen Sie die Online-Hilfe:

1. Klicken Sie auf der Symbolleiste auf "Hilfe", um die Online-Hilfe für CA Enterprise Log Manager zu öffnen.

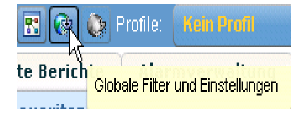
   

   Das CA Enterprise Log Manager-Hilfesystem wird geöffnet. Im linken Fensterbereich wird der Inhalt aufgelistet.

2. Öffnen Sie über eine Hilfe-Schaltfläche die kontextabhängige Hilfe (siehe folgendes Beispiel).

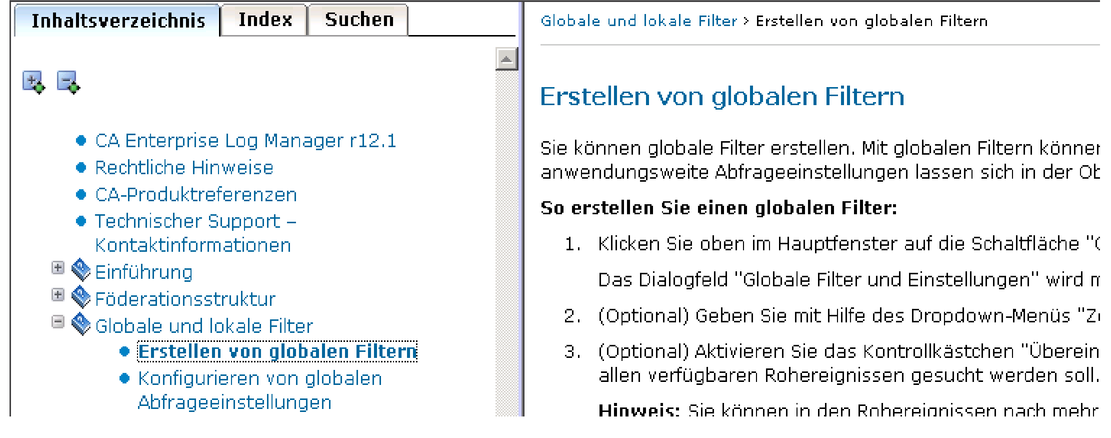
   a. Klicken Sie auf die Schaltfläche "Globale Filter anzeigen/bearbeiten".

Das Fenster "Globale Filter und Einstellungen" mit einer Hilfe-Schaltfläche wird geöffnet.



b. Klicken Sie auf die Schaltfläche "Hilfe". In einem zweiten Fenster wird die Online-Hilfe für den Vorgang geöffnet, den Sie auf der aktuellen Seite, im aktuellen Bereich oder im Dialogfeld durchführen können.



c. Wenn Sie wissen, welche Aufgabe Sie ausführen möchten, aber nicht wissen, wie Sie in CA Enterprise Log Manager auf die entsprechende Seite gelangen, nutzen Sie zunächst das Inhaltsverzeichnis. Durch Klicken auf den Aufgabennamen wird die Seite geöffnet.

Hinweis: Wenn Sie die Aufgabe im Inhaltsverzeichnis nicht finden können, schlagen Sie im Bookshelf der Dokumentation nach.

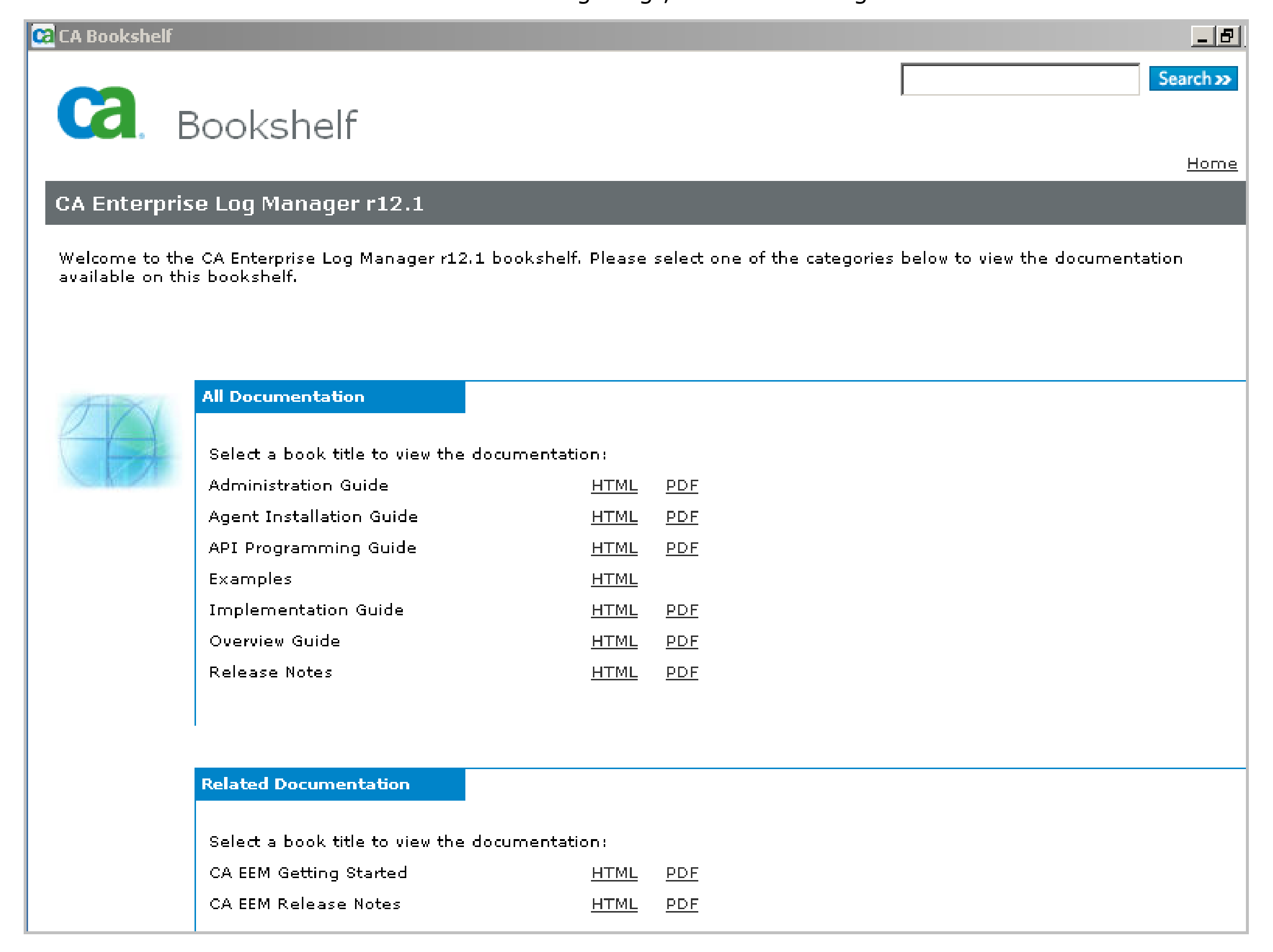
Überblick über das Bookshelf mit Dokumentation

Sie können das Bookshelf auf Ihr lokales Laufwerk kopieren. Die Bücher können als HTML oder PDF geöffnet werden. Bücher im HTML-Format enthalten buchübergreifende Querverweise.

So erhalten Sie einen Überblick über das Bookshelf:

1. Kopieren Sie das Bookshelf von der Installations-DVD der Anwendung auf Ihr lokales Laufwerk oder laden Sie es von der CA Kundensupport-Website herunter. Doppelklicken Sie auf die Datei "Bookshelf.hta" oder "Bookshelf.html", um das Bookshelf zu öffnen.

   Ein Fenster wird angezeigt, das in etwa folgendermaßen aussieht:



Eine Beschreibung des Inhalts der wichtigsten Handbücher und Beispiele folgen:

Komponente	Inhalt
Agent-Installationshandbuch	Installieren der Agents
Implementierungshandbuch	Installieren und Konfigurieren eines CA Enterprise Log Manager-Systems.
Administrationshandbuch	Anpassen der Konfiguration, Durchführen von routinemäßigen Verwaltungsaufgaben und Arbeiten mit Abfragen, Berichten und Alarmen.
API-Programmierhandbuch	Mit der API können Sie Ereignisdaten in einem Web-Browser anzeigen oder Berichte in ein anderes CA-Produkt oder ein Produkt eines Drittanbieters einbetten.
Beispiele	Lösen allgemeiner unternehmensbezogener Probleme mit Verknüpfungen zu Kapiteln in der Dokumentation.

2. Geben Sie im Eingabefeld "Suchen" einen Wert ein, und klicken Sie auf die Schaltfläche "Suchen", um alle dokumentierten Vorkommnisse anzuzeigen, die Ihren Eintrag enthalten.
3. Klicken Sie auf eine Druckverknüpfung, um die PDF-Version des ausgewählten Handbuchs zu öffnen.
4. Klicken Sie auf eine HTML-Verknüpfung, um den integrierten Dokumentationssatz zu öffnen. Der integrierte Satz enthält alle Handbücher im HTML-Format. Wenn Sie die HTML-Verknüpfung für das Übersichtshandbuch wählen, wird dieses Handbuch angezeigt.



Terminologieglossar

Abfrage

Eine *Abfrage* ist ein Satz von Kriterien, mit denen die Ereignisprotokollspeicher der aktiven CA Enterprise Log Manager-Server und, sofern angegeben, seiner föderierten Server durchsucht werden. Eine Abfrage richtet sich an die heißen, warmen oder verfügbaren gemachten Datenbanken, die in der Where-Klausel der Abfrage angegeben wurden. Beispiel: Wenn die Where-Klausel die Abfrage auf Ereignisse mit source_username="myname" in einem bestimmten Zeitrahmen beschränkt und nur zehn von 1000 Datenbanken Datensätze enthalten, die diesen Kriterien (basierend auf den Informationen in der Katalogdatenbank) entsprechen, wird die Abfrage nur in diesen zehn Datenbanken durchgeführt. Eine Abfrage kann maximal 5000 Datenzeilen zurückgeben. Ein Benutzer mit einer vordefinierten Rolle kann eine Abfrage durchführen. Nur Analysten und Administratoren können eine Abfrage planen, um einen Aktionsalarm zu verteilen, einen Bericht unter Auswahl der enthaltenen Abfragen erstellen oder eine benutzerdefinierte Abfrage mithilfe des Abfragedesign-Assistenten erstellen. Siehe auch Archivabfrage.

Abfragebibliothek

Die *Abfragebibliothek* ist der Speicher für alle vordefinierten und benutzerdefinierten Abfragen, Abfragekennungen und Prompt-Filter.

Administratorrolle

Die *Administratorrolle* erteilt Benutzern die Berechtigung, alle gültigen Aktionen in allen Ressourcen von CA Enterprise Log Manager auszuführen. Nur Administratoren dürfen Protokollerfassung und Services konfigurieren oder Benutzer, Zugriffsrichtlinien und Zugriffsfilter verwalten.

Agent

Ein *Agent* ist ein generischer Service, der mit Connectors konfiguriert wurde, von denen jeder Rohereignisse von einer einzelnen Ereignisquelle erfasst und diese dann zur Verarbeitung an CA Enterprise Log Manager sendet. Jeder CA Enterprise Log Manager verfügt über einen integrierten Agent. Außerdem können Sie einen Agenten auf einem Remote-Sammelpunkt installieren und Ereignisse auf Hosts erfassen, auf denen keine Agenten installiert werden können. Sie können einen Agenten auch auf dem Host installieren, auf dem die Ereignisquellen ausgeführt werden, und so die Möglichkeit nutzen, für einen CA Enterprise Log Manager Unterdrückungsregeln anzuwenden und Übertragungen zu verschlüsseln.

Agenten-Explorer

Der *Agenten-Explorer* bezeichnet den Speicher für die Einstellungen der Agentenkonfiguration. (Agenten können in einem Erfassungspunkt oder in Endpunkten installiert werden, an denen Ereignisquellen vorhanden sind.)

Agentengruppe

Eine *Agentengruppe* ist eine Kennung, die Benutzer auf ausgewählte Agenten anwenden können, mit denen Benutzer eine Agentenkonfiguration gleichzeitig auf mehrere Agenten anwenden und Berichte auf der Basis der Gruppen abrufen können. Ein bestimmter Agent kann jeweils nur zu einer Gruppe gehören. Agentengruppen basieren auf benutzerdefinierten Kriterien wie der geografischen Region oder der Wichtigkeit.

Agenten-Management

Agenten-Management ist der Software-Prozess, der alle Agenten steuert, die mit allen föderierten CA Enterprise Log Managers verknüpft sind. Dabei werden die Agenten, mit denen kommuniziert wird, authentifiziert.

Aktionsabfrage

Eine *Aktionsabfrage* ist eine Abfrage, die einen Aktionsalarm unterstützt. Sie wird in einem wiederkehrenden Plan ausgeführt, um die Bedingungen zu testen, die von dem zugehörigen Aktionsalarm definiert sind.

Aktionsalarm

Ein *Aktionsalarm* ist ein geplanter Abfragejob, mit dessen Hilfe Richtlinienverletzungen, Nutzungstrends, Anmeldemuster und andere Ereignisaktionen, die ein kurzfristiges Eingreifen erfordern, ermittelt werden können. Wenn Alarmabfragen Ergebnisse zurückgeben, werden diese standardmäßig auf der Seite "Alarme" in CA Enterprise Log Manager angezeigt und außerdem einem RSS-Feed hinzugefügt. Wenn Sie einen Alarm planen, können Sie zusätzliche Ziele angeben, einschließlich E-Mail, einen CA IT PAM-Ereignis-/Alarmausgabeprozess und SNMP-Traps.

Alarmserver

Der *Alarmserver* ist der Speicher für Aktionsalarme und Aktionsalarmjobs.

Analystenrolle

Die *Analystenrolle* erteilt Benutzern die Berechtigung, benutzerdefinierte Berichte und Abfragen zu erstellen, Berichte zu bearbeiten und Anmerkungen dazu einzugeben, Kennungen zu erstellen und Berichte und Aktionswarnungen zu planen. Analysten können auch alle Auditor-Aufgaben durchführen.

Anwendungsbenutzer

Ein *Anwendungsbenutzer* ist ein globaler Benutzer, dem Detaildaten auf Anwendungsebene zugewiesen wurden. Zu den CA Enterprise Log Manager-Anwendungsbenutzerdetails gehören die Benutzergruppe und Einschränkungen der Zugriffsrechte. Wenn der Benutzerspeicher das lokale Repository ist, umfassen die Anwendungsbenutzerdetails auch die Anmeldedaten und die Kennwortrichtlinien.

Anwendungsgruppe

Eine *Anwendungsgruppe* ist eine produktspezifische Gruppe, die einem globalen Benutzer zugewiesen werden kann. Vordefinierte Anwendungsgruppen für CA Enterprise Log Manager oder Rollen sind "Administrator", "Analyst" und "Auditor". Diese Anwendungsgruppen stehen nur CA Enterprise Log Manager-Benutzern zur Verfügung. Sie können Benutzern anderer Produkte, die auf demselben CA EEM-Server registriert wurden, nicht zugewiesen werden. Benutzerdefinierte Anwendungsgruppen müssen zur Standardrichtlinie für den CALM-Anwendungszugriff hinzugefügt werden, damit die Benutzer auf CA Enterprise Log Manager zugreifen können.

Anwendungsinstanz

Eine *Anwendungsinstanz* ist ein allgemeiner Bereich imCA EEM-Repository, in dem alle Berechtigungsrichtlinien, Benutzer, Gruppen, Inhalte und Konfigurationen gespeichert werden. Normalerweise verwenden alle CA Enterprise Log Manager-Server in einem Unternehmen dieselbe Anwendungsinstanz (standardmäßig CAELM). Sie können CA Enterprise Log Manager-Server mit verschiedenen Anwendungsinstanzen installieren, aber nur die Server, die dieselbe Anwendungsinstanz gemeinsam nutzen, können föderiert werden. Server, die für die Verwendung desselben CA EEM-Servers, aber mit verschiedenen Anwendungsinstanzen konfiguriert wurden, nutzen nur den Benutzerspeicher, die Kennwortrichtlinien und die globalen Gruppen gemeinsam. Verschiedene CA-Produkte verfügen über verschiedene Standardanwendungsinstanzen.

Anwendungsressource

Eine *Anwendungsressource* ist eine der CA Enterprise Log Manager-spezifischen Ressourcen, in denen CALM-Zugriffsrichtlinien bestimmten Identitäten die Durchführung bestimmter anwendungsspezifischer Aktionen (wie der Erstellung, Planung und Bearbeitung) gewähren oder verweigern. Beispiele hierfür sind Berichte, Alarme und Integration. Sieh auch globale Ressource.

AppObjects

AppObjects oder Anwendungsobjekte sind produktspezifische Ressourcen, die in CA EEM unter der Anwendungsinstanz eines bestimmten Produkts gespeichert sind. Für die CAELM-Anwendungsinstanz umfassen diese Ressourcen Berichts- und Abfrageinhalte, geplante Berichts- und Alarmjobs, Agenteninhalte und -konfigurationen, Service-, Adapter- und Integrationskonfigurationen, Datenzuordnungs- und Nachrichtenanalysedateien sowie Unterdrückungs- und Zusammenfassungsregeln.

Archivabfrage

Eine *Archivabfrage* ist eine Abfrage des Katalogs, anhand dessen die kalten Datenbanken identifiziert werden, die wiederhergestellt und für die Abfrage verfügbar gemacht werden müssen. Eine Archivabfrage unterscheidet sich darin von einer normalen Abfrage, dass sie sich auf kalte Datenbanken bezieht, während sich normale Abfragen auf heiße, warme und verfügbar gemachte Datenbanken beziehen. Administratoren können eine Archivabfrage über die Registerkarte "Verwaltung", die Unterregisterkarte "Protokollerfassung" und die Option "Archivkatalogabfrage" starten.

Archivierte Datenbanken

Die *archivierten Datenbanken* auf einem bestimmten CA Enterprise Log Manager-Server umfassen alle warmen Datenbanken, die für die Abfrage zur Verfügung stehen, jedoch manuell gesichert werden müssen, bevor sie ablaufen, alle kalten Datenbanken, die als gesichert erfasst wurden, und alle Datenbanken, die als von einer Datensicherung wiederhergestellt erfasst wurden.

Archivkatalog

Siehe Katalog.

Assistent für Analysedateien

Der *Assistent für Analysedateien* ist eine CA Enterprise Log Manager-Funktion, mit der Administratoren XMP-Dateien (eXtensible Message Parsing), die auf dem CA Enterprise Log Manager-Verwaltungsserver gespeichert werden, erstellen, bearbeiten und analysieren können. Die Anpassung der Analyse eingehender Ereignisdaten umfasst auch die Bearbeitung vorabgestimmter Zeichenfolgen und Filter. Neue und bearbeitete Dateien werden im Protokollerfassung-Explorer, in der Ereignisverfeinerungsbibliothek, in den Analysedateien und im Benutzerordner angezeigt.

Audit-Datensätze

Audit-Datensätze enthalten Sicherheitsereignisse, wie Authentifizierungsversuche, Dateizugriffe und Änderungen an Sicherheitsrichtlinien, Benutzerkonten und Benutzerrechten. Administratoren geben an, welche Ereignistypen auditiert und welche protokolliert werden sollten.

Auditorenrolle

Die *Auditorenrolle* gewährt den Benutzern Zugriff auf Berichte und die darin enthaltenen Daten. Auditoren können Berichte, die Listen mit den Berichtvorlagen, den geplanten Berichtaufträgen und mit den generierten Berichten anzeigen. Auditoren können Berichte planen und mit Anmerkungen versehen. Auditoren haben keinen Zugriff auf die RSS-Feeds (Rich Site Summary), außer die Konfiguration erfordert keine Authentifizierung für die Anzeige von Aktionsalarmen.

Aufgezeichnetes Ereignis

Ein *aufgezeichnetes Ereignis* bezeichnet die Informationen des Rohereignisses oder des verfeinerten Ereignisses, nachdem diese in die Datenbank eingefügt wurden. Rohereignisse werden immer als verfeinerte Ereignisse erfasst, außer sie wurden unterdrückt oder zusammengefasst. Diese Informationen werden gespeichert und können durchsucht werden.

Auto-Archivierung

Auto-Archivierung ist ein konfigurierbarer Prozess, der das Verschieben von Archivdatenbanken von einem Server zu einem anderen automatisiert. In der ersten Phase der Auto-Archivierung sendet der Erfassungsserver neu archivierte Datenbanken in der von Ihnen angegebenen Häufigkeit zum Berichtsserver. In der zweiten Phase der Auto-Archivierung sendet der Berichtsserver ältere Datenbanken zur langfristigen Speicherung an den Remote-Speicher, wodurch die Notwendigkeit eines manuellen Sicherungs- und Verschiebevorgangs entfällt. Für die Auto-Archivierung müssen Sie eine Authentifizierung ohne Kennwörter vom Quell- zum Zielserver konfigurieren.

Automatische Software-Updates

Automatische Software-Updates betreffen binäre und nicht-binäre Dateien, die vom CA-Server für automatische Software-Updates zur Verfügung gestellt werden. Binärdateien sind Produktmodulaktualisierungen, die normalerweise in CA Enterprise Log Manager installiert sind. Nicht-binäre Dateien oder Inhaltsaktualisierungen werden auf dem Management-Server gespeichert.

Benutzergruppe

Eine *Benutzergruppe* kann eine Anwendungsgruppe, eine globale oder eine dynamische Gruppe sein. Vordefinierte CA Enterprise Log Manager-Anwendungsgruppen sind Administrator, Analyst und Auditor. CA Enterprise Log Manager-Benutzer können über Mitgliedschaften außerhalb von CA Enterprise Log Manager zu globalen Gruppen gehören. Dynamische Gruppen sind benutzerdefiniert und werden über eine dynamische Gruppenrichtlinie erstellt.

Benutzername "EiamAdmin"

EiamAdmin ist der Standardname für den Superuser, der dem Benutzer zugewiesen wird, der die CA Enterprise Log Manager-Server installiert. Bei der Installation der ersten CA Enterprise Log Manager-Software erstellt der Installierende ein Kennwort für dieses Superuser-Konto, wenn nicht bereits ein Remote-CA EEM-Server vorhanden ist. In diesem Fall muss der Installierende das vorhandene Kennwort eingeben. Nach der Installation der Soft-Appliance öffnet der Installierende einen Browser von einer Workstation aus, gibt die URL für CA Enterprise Log Manager ein und meldet sich als "EiamAdmin" mit dem zugehörigen Kennwort an. Dieser erste Benutzer richtet den Benutzerspeicher ein, erstellt Kennwortrichtlinien sowie das erste Benutzerkonto mit Administratorrolle. Optional kann der Benutzer "EiamAdmin" jede Operation durchführen, die von CA EEM gesteuert wird.

Benutzerrolle

Eine *Benutzerrolle* kann eine vordefinierte oder eine benutzerdefinierte Anwendungsgruppe sein. Benutzerdefinierte Benutzerrollen werden benötigt, wenn die vordefinierten Anwendungsgruppen (Administrator, Analyst und Auditor) nicht ausreichend differenziert sind, um Arbeitszuweisungen zu reflektieren. Für benutzerdefinierte Benutzerrollen sind benutzerdefinierte Zugriffsrichtlinien erforderlich. Zudem muss vordefinierten Richtlinien die neue Rolle hinzugefügt werden.

Benutzerspeicher

Ein *Benutzerspeicher* ist das Repository für globale Benutzerinformationen und Kennwortrichtlinien. Der CA Enterprise Log Manager-Benutzerspeicher ist standardmäßig das lokale Repository, das jedoch so konfiguriert werden kann, dass CA SiteMinder oder ein unterstütztes LDAP-Verzeichnis wie Microsoft Active Directory, Sun One oder Novell eDirectory referenziert werden. Unabhängig davon, wie der Benutzerspeicher konfiguriert wird, enthält das lokale Repository auf dem Management-Server anwendungsspezifische Informationen über die Benutzer, wie ihre Benutzerrolle und dazugehörige Zugriffsrichtlinien.

Beobachtetes Ereignis

Ein *beobachtetes Ereignis* ist ein Ereignis, das eine Quelle, ein Ziel und einen Agenten umfasst, wobei das Ereignis von einem Ereigniserfassungsagenten beobachtet und erfasst wird.

Bericht

Ein *Bericht* ist eine grafische oder tabellarische Darstellung von Ereignisprotokolldaten, die beim Ausführen von vordefinierten oder benutzerdefinierten Abfragen mit Filtern erstellt wird. Die Daten können aus heißen, warmen und verfügbar gemachten Datenbanken im Ereignisprotokollspeicher des ausgewählten Servers und, sofern angefordert, der zugehörigen föderierten Server stammen.

Berichtsbibliothek

Die *Berichtsbibliothek* ist der Speicher für alle vordefinierten und benutzerdefinierten Berichte, Berichtskennungen und geplanten Berichtsjobs.

Berichtsserver

Der *Berichtsserver* ist der Service, der folgenden Konfigurationsinformationen speichert: den beim Mailen von Alarmen zu verwendenden E-Mail-Server, die Anzeige von Berichten, die im PDF-Format gespeichert werden, und die Beibehaltung von Richtlinien für Berichte, die auf dem Berichtsserver gespeichert werden, sowie von Alarmen, die an den RSS-Feed gesendet werden.

Berichtsserver

Ein *Berichtsserver* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Ein Berichtsserver empfängt automatisch archivierte warme Datenbanken von einem oder mehreren Erfassungsservern. Ein Berichtsserver verwaltet Abfragen, Berichte, geplante Alarme und geplante Berichte.

CA Enterprise Log Manager

CA Enterprise Log Manager ist ein Lösung, mit der Sie Protokolle weit verteilter Ereignisquellen verschiedenster Art sammeln, nach Übereinstimmungen von Abfragen und Berichten suchen und Datensätze von Datenbanken mit komprimierten Protokollen speichern können, die Sie in externe Langzeitspeicher verschoben haben.

CA IT PAM

CA IT PAM ist die Abkürzung für CA IT Process Automation Manager. Dieses CA-Produkt automatisiert von Ihnen definierte Prozesse. CA Enterprise Log Manager verwendet zwei Prozesse: den Prozess zur Erstellung eines Ereignis-/Alarmausgabeprozesses für ein lokales Produkt, wie z. B. CA Service Desk, und den Prozess zur dynamischen Erstellung von Listen, die als Schlüsselwerte importiert werden können. Für die Integration ist CA IT PAM r2.1 erforderlich.

CA Spectrum

CA Spectrum ist ein Neztwerkfehlerverwaltungsprogramm, das in CA Enterprise Log Manager integriert werden kann, um als Ziel für Alarme in Form von SNMP-Traps zu dienen.

CA-Adapter

Die *CA-Adapter* sind eine Gruppe von Listenern, die Ereignisse von CA Audit-Komponenten erhalten. Diese Komponenten umfassen CA Audit-Clients, iRecorder und SAPI-Recorder sowie Quellen, die Ereignisse nativ über iTechnology senden.

CAELM

CAELM ist der Name der Anwendungsinstanz, die CA EEM für CA Enterprise Log Manager verwendet. Um die CA Enterprise Log Manager-Funktionen in CA Embedded Entitlements Manager aufzurufen, geben Sie die URL "https://<ip_address>:5250/spin/eiam/eiam.csp" ein, dann wählen Sie "CAELM" als Anwendungsnamen und geben das Kennwort des Benutzers "EiamAdmin" ein.

caelmadmin

Der Benutzername und das Kennwort *caelmadmin* sind Anmeldeinformationen, die für den Zugriff auf das Betriebssystem der Soft-Appliance benötigt werden. Die Benutzerkennung "caelmadmin" wird während der Installation des Betriebssystems erstellt. Während der Installation der Software-Komponente muss der Installierende das Kennwort für das CA EEM-Superuser-Konto, EiamAdmin, eingeben. Dem Konto "caelmadmin" wird dasselbe Konto zugewiesen. Es empfiehlt sich, dass sich der Server-Administrator über "ssh" als "caelmadmin"-Benutzer anmeldet und dieses Kennwort ändert. Auch wenn der Administrator sich nicht über "ssh" als Root anmelden kann, kann er bei Bedarf Benutzer zu "Root" (su root) wechseln lassen.

caelmservice

Der *caelmservice* bezeichnet eine Service-Konto, das es ermöglicht, dass iGateway und die lokalen CA EEM-Services als Nicht-Root-Benutzer ausgeführt werden können. Das caelmservice-Konto wird für die Installation von Betriebssystemaktualisierungen verwendet, die mit automatischen Software-Updates heruntergeladen werden.

CALM

CALM ist eine vordefinierte Ressourcenklasse, die folgende CA Enterprise Log Manager-Ressourcen umfasst: Alarm, ArchiveQuery, calmTag, Daten, EventGrouping, Integration und Bericht. Folgende Aktionen sind in dieser Ressourcenklasse zulässig: Anmerken (Berichte), Erstellen (Alarm, calmTag, EventGrouping, Integration und Bericht), Datenzugriff (Daten), Ausführen (ArchiveQuery) und Planen (Alarm, Bericht).

CALM-Anwendungszugriffsrichtlinie

Die *CALM-Anwendungszugriffsrichtlinie* ist ein Zugriffssteuerungslistentyp einer Richtlinie zur Bereichsdefinierung, die festlegt, wer sich in CA Enterprise Log Manager anmelden darf. Anmeldungszugriff wird standardmäßig dem [Gruppen-]Administrator, dem [Gruppen-] Analysen und dem [Gruppen-]Auditor erteilt.

calmTag

calmTag ist ein benanntes Attribut für das Anwendungsobjekt, das bei der Erstellung einer Richtlinie zur Bereichsdefinierung verwendet wird, um Benutzer auf bestimmte Berichte und Abfragen zu beschränken, die zu bestimmten Kennungen gehören. Alle Berichte und Abfrage sind Anwendungsobjekte und haben "calmTag" als Attribut. (Dies ist nicht zu verwechseln mit der Ressource "Kennung".)

CA-Server für automatische Software-Updates

Der *CA-Server für automatische Software-Updates* ist die Quelle für automatische Aktualisierungen aus CA.

CEG-Felder

CEG-Felder sind Label, mit denen die Darstellung von Rohereignisfeldern aus unterschiedlichen Ereignisquellen standardisiert wird. Während der Verfeinerung von Ereignissen wandelt CA Enterprise Log Manager Rohereignismeldungen in Namen-/Wertepaare um und ordnet die Namen der Rohereignisse Standard-CEG-Feldern zu. Bei dieser Verfeinerung entstehen Namen-/Wertepaare, die aus CEG-Feldern und -Werten aus dem Rohereignis bestehen. So werden unterschiedliche Labels aus Rohelementen für dasselbe Datenobjekt oder Netzwerkelement bei der Verfeinerung von Rohereignissen in denselben CEG-Feldnamen umgewandelt. CEG-Felder werden in der MIB der SNMP-Traps bestimmten OIDs zugeordnet.

Client für automatische Software-Updates

Ein *Client für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server, der Inhaltsaktualisierungen von einem anderen CA Enterprise Log Manager-Server erhält, der als Proxy-Server für automatische Software-Updates bezeichnet wird. Clients für automatische Software-Updates fragen den konfigurierten Proxy-Server in regelmäßigen Abständen ab und rufen neue Aktualisierungen bei Verfügbarkeit ab. Nach dem Abrufen der Aktualisierungen installiert der Client die heruntergeladenen Komponenten.

Computersicherheitsprotokoll-Verwaltung

Die *Computersicherheitsprotokoll-Verwaltung* wird durch NIST als "der Prozess zum Generieren, Übertragen, Speichern, Analysieren und Entsorgen von Computersicherheitsprotokoll-Daten" definiert.

Connector

Ein *Connector* ist eine Integration für eine bestimmte Ereignisquelle, die in einem bestimmten Agenten konfiguriert wurde. Ein Agent kann mehrere Connectors ähnlicher oder verschiedener Typen in den Speicher laden. Der Connector ermöglicht die Erfassung von Rohereignissen von einer Ereignisquelle und die regelbasierte Übertragung konvertierter Ereignisse in einen Ereignisprotokollspeicher, wo sie in die heiße Datenbank eingefügt werden. Standardisierte Integrationen liefern eine optimierte Erfassung einer breiten Palette von Ereignisquellen, einschließlich Betriebssystemen, Datenbanken, Webservern, Firewalls und diversen Arten von Sicherheitsanwendungen. Sie können einen Connector für eine selbstentwickelte Ereignisquelle von Anfang an selbst definieren, oder Sie verwenden eine Integration als Vorlage.

Datenbankstatus "heiß"

Der *Datenbankstatus "heiß"* bezeichnet den Status der Datenbank im Ereignisprotokollspeicher, wenn neue Ereignisse eingefügt werden. Wenn die heiße Datenbank eine konfigurierbare Größe auf dem Erfassungsserver erreicht, wird sie komprimiert, katalogisiert und in den warmen Speicher auf dem Berichtsserver verschoben. Außerdem speichern alle Server neue selbstüberwachende Ereignisse in einer heißen Datenbank.

Datenbankstatus "kalt"

Der *Datenbankstatus "kalt"* wird einer warmen Datenbank zugewiesen, wenn ein Administrator das Hilfsprogramm "LMArchive" ausführt, um CA Enterprise Log Manager zu benachrichtigen, dass die Datenbank gesichert wurde. Administratoren müssen warmen Datenbanken sichern und dieses Hilfsprogramm ausführen, bevor die Datenbanken gelöscht werden. Eine warme Datenbank wird automatisch gelöscht, wenn ihr Alter den für "Maximale Anzahl an Archivtagen" konfigurierten Wert erreicht oder wenn der für "Festplattenspeicher für Archiv" konfigurierte Schwellenwert erreicht wird, je nachdem, welcher Wert zuerst erreicht wird. Sie können die Archivdatenbank abfragen, um kalte und warme Datenbanken zu ermitteln.

Datenbankstatus "verfügbar gemacht"

Der *Datenbankstatus "verfügbar gemacht"* ist der Status, der einer Datenbank zugewiesen wird, die im Archivverzeichnis wiederhergestellt wurde, nachdem der Administrator das Hilfsprogramm "LMArchive" ausgeführt hat, um CA Enterprise Log Manager mitzuteilen, dass die Datenbank wiederhergestellt wurde. Verfügbar gemachte Datenbanken bleiben für die Anzahl der Stunden erhalten, die für die Exportrichtlinie konfiguriert wurde. Ereignisprotokolle können in Datenbanken mit dem Status "heiß", "warm" und "verfügbar gemacht" abgefragt werden.

Datenbankstatus "warm"

Der *Datenbankstatus "warm"* bezeichnet den Status, in dem eine heiße Datenbank von Ereignisprotokollen verschoben wird, wenn die Größe (Maximale Zeilenanzahl) der heißen Datenbank überschritten wird oder wenn nach der Wiederherstellung einer kalten Datenbank in einem neuen Ereignisprotokollspeicher eine Neukatalogisierung durchgeführt wird. Warme Datenbanken werden komprimiert und im Ereignisprotokollspeicher beibehalten, bis ihr Alter (in Tagen) den konfigurierten Wert für "Maximale Anzahl an Archivtagen" überschreitet. Ereignisprotokolle können in Datenbanken mit dem Status "heiß", "warm" und "verfügbar gemacht" abgefragt werden.

Datenbankstatuswerte

Es gibt folgende *Datenbankstatuswerte:* "heiß" für eine nicht komprimierte Datenbank mit neuen Ereignissen, "warm" für eine Datenbank mit komprimierten Ereignissen, "kalt" für eine gesicherte Datenbank und "verfügbar gemacht" für eine Datenbank, die im Ereignisprotokollspeicher wiederhergestellt wurde, auf dem sie gesichert wurde. Sie können heiße, warme und verfügbar gemachte Datenbanken abfragen. Eine Archivabfrage zeigt die Informationen von kalten Datenbanken an.

Datenzugriff

Datenzugriff ist eine Art der Berechtigung, die allen CA Enterprise Log Managers über die Standarddatenzugriffsrichtlinie in der CALM-Ressourcenklasse gewährt wird. Alle Benutzer haben Zugriff auf alle Daten, außer wenn diese durch Datenzugriffsfilter eingeschränkt sind.

Datenzuordnung

Datenzuordnung ist der Prozess der Zuordnung der Schlüsselwertpaare in CEG. Die Datenzuordnung wird durch eine DM-Datei gesteuert.

Datenzuordnung von Dateien

Unter der *Datenzuordnung von Dateien* versteht man XML-Dateien, die die CA-ELM-Schemadefinition (CEG) verwenden, um Ereignisse vom Ursprungsformat in ein CEG-kompatibles Format zu übertragen, das zur Berichterstellung und Analyse im Ereignisprotokollspeicher gespeichert werden kann. Für jeden Protokollnamen wird eine Datenzuordnungsdatei benötigt, bevor die Ereignisdaten gespeichert werden können. Die Benutzer können eine Kopie der Datenzuordnungsdatei ändern und diese auf einen angegebenen Connector anwenden.

Delegierungsrichtlinie

Eine *Delegierungsrichtlinie* ist eine Zugriffsrichtlinie, mit der ein Benutzer seine Rechte auf einen anderen Benutzer, eine andere Anwendungsgruppe, eine andere globale oder dynamische Gruppe übertragen kann. Delegierungsrichtlinien, die von einem gelöschten oder deaktivierten Benutzer erstellt wurden, müssen explizit gelöscht werden.

Direkte Protokollerfassung

Direkte Protokollerfassung bezeichnet die Protokollerfassungsmethode, bei der es keinen unmittelbaren Agenten zwischen Ereignisquelle und der CA Enterprise Log Manager-Software gibt.

Dynamische Benutzergruppe

Eine *dynamische Benutzergruppe* setzt sich aus globalen Benutzern zusammen, die ein oder mehrere Attribute gemeinsam haben. Eine dynamische Benutzergruppe wird über eine spezielle Richtlinie für dynamische Benutzergruppen erstellt, wobei der Ressourcenname der Name der dynamischen Benutzergruppe ist und die Mitgliedschaft auf einer Gruppe von Filtern basiert, die anhand von Benutzer- und Gruppenattributen erstellt wird.

EEM-Benutzer

Der *EEM-Benutzer*, der im Auto-Archivierungsbereich des Ereignisprotokollspeichers konfiguriert wird, gibt den Benutzer an, der eine Archivabfrage durchführen, die Archivdatenbank neu katalogisieren, das Hilfsprogramm "LMArchive" und das Shellskript "restore-ca-elm" zur Wiederherstellung von Archivdatenbanken zur Prüfung ausführen kann. Dem Benutzer muss die vordefinierte Rolle des Administrators oder eine benutzerdefinierte Rolle mit einer benutzerdefinierten Richtlinie zugewiesen werden, die die Aktion "Bearbeiten" in der Datenbankressource zulässt.

Eingabeaufforderung

Eine *Eingabeaufforderung* ist ein besonderer Typ von Abfrage, durch die Ergebnisse basierend auf dem eingegebenen Wert und den ausgewählten CEG-Feldern angezeigt werden. Es werden nur Zeilen für Ereignisse zurückgegeben, bei denen der eingegebene Wert in mindestens einem der ausgewählten CEG-Felder angezeigt wird.

ELM-Schemadefinition (CEG)

Die *ELM-Schemadefinition* ist das Schema, das ein Standardformat enthält, in das CA Enterprise Log Manager-Ereignisse mithilfe von Analysen und Zuordnungen konvertiert werden, bevor diese im Ereignisprotokollspeicher gespeichert werden. CEG verwendet allgemeine, normalisierte Felder, um die Sicherheitsereignisse von verschiedenen Plattformen und Produkten zu definieren. Ereignisse, die nicht analysiert oder zugeordnet werden können, werden als Rohereignisse gespeichert.

EPHI-Berichte

Die *EPHI-Berichte* sind Berichte, die sich auf die HIPAA-Sicherheit beziehen, wobei EPHI für Electronic Protected Health Information (Elektronisch geschützte Gesundheitsinformationen) steht. Mit diesen Berichten können Sie einfach demonstrieren, dass alle einzeln feststellbaren Gesundheitsinformationen der Patienten, die elektronisch erstellt, verwaltet oder übertragen werden, auch geschützt sind.

Ereignis-/Alarmausgabeprozess

Der *Ereignis-/Alarmausgabeprozess* ist der IT PAM-Prozess von CA, durch den ein Produkt eines anderen Herstellers aufgerufen wird, um auf Alarmdaten zu reagieren, die in CA Enterprise Log Manager konfiguriert werden. Sie können einen CA IT PAM-Prozess beim Planen eines Alarmjobs als Ziel auswählen. Wenn ein Alarm zur Ausführung des CA IT PAM-Prozesses führt, sendet CA Enterprise Log Manager CA IT PAM-Alarmdaten. CA IT PAM leitet diese zusammen mit eigenen Verarbeitungsparametern als Teil des Ereignis-/Alarmausgabeprozesses an das Produkt des anderen Herstellers weiter.

Ereignisaggregation

Unter *Ereignisaggregation* versteht man den Prozess, in dem ähnliche Protokolleinträge in einen Eintrag konsolidiert werden, der die Anzahl der Vorkommnisse des Ereignisses enthält. Über Zusammenfassungsregeln wird definiert, wie Ereignisse aggregiert werden.

Ereignisaktion (event_action)

Die *Ereignisaktion* ist das ereignisspezifische Feld auf der vierten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es beschreibt allgemeine Aktionen. Beispieltypen für Ereignisaktionen sind Start und Stopp eines Prozesses oder Anwendungsfehler.

Ereigniserfassung

Ereigniserfassung bezeichnet das Lesen der Rohereigniszeichenfolge aus einer Ereignisquelle und das Senden dieser an den konfigurierten CA Enterprise Log Manager. Auf die Ereigniserfassung folgt die Ereignisverfeinerung.

Ereignisfilterung

Ereignisfilterung ist der Prozess, in dem Ereignisse auf der Basis von CEG-Filtern verworfen werden.

Ereigniskategorie (event_category)

Die *Ereigniskategorie* ist das ereignisspezifische Feld auf der zweiten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es dient der weiteren Klassifizierung von Ereignissen mit einen speziellen Idealmodell. Ereigniskategorietypen umfassen die Betriebssicherheit, das Identitäten-Management, das Konfigurations-Management, den Ressourcen- und Systemzugriff.

Ereigniskategorien

Ereigniskategorien sind Kennungen, anhand derer CA Enterprise Log Manager-Ereignisse nach ihrer Funktion klassifiziert, bevor sie in den Ereignisspeicher eingefügt werden.

Ereignisklasse (event_class)

Die *Ereignisklasse* ist das ereignisspezifische Feld auf der dritten Ebene der Ereignisnormalisierung, das von CEG verwendet wird. Es dient der weiteren Klassifizierung von Ereignissen mit einer speziellen Ereigniskategorie.

Ereignisprotokollspeicher

Der *Ereignisprotokollspeicher* ist eine Komponente im CA Enterprise Log Manager-Server, bei der eingehende Ereignisse in Datenbanken gespeichert werden. Die Datenbanken im Ereignisprotokollspeicher müssen vor dem Zeitpunkt, der für den Löschvorgang konfiguriert wurde, manuell gesichert werden und zu einer Remote-Protokollspeicherlösung verschoben werden. Archivierte Datenbanken können in einem Ereignisprotokollspeicher wiederhergestellt werden.

Ereignisprotokollspeicher

Der Ereignisprotokollspeicher ist das Ergebnis des Archivierungsprozesses, bei dem der Benutzer eine warme Datenbank sichert, CA Enterprise Log Manager durch Ausführen des Hilfsprogramms "LMArchive" benachrichtigt und die gesicherte Datenbank aus dem Ereignisprotokollspeicher in den langfristigen Speicher verschiebt.

Ereignisquelle

Eine *Ereignisquelle* ist der Host, von dem ein Connector Rohereignisse erfasst. Eine Ereignisquelle kann mehrere Protokollspeicher enthalten, auf die jeweils durch einen separaten Connector zugegriffen wird. Die Bereitstellung eines neuen Connectors umfasst gewöhnlich die Konfiguration der Ereignisquelle, so dass der Agent darauf zugreifen und Rohereignisse aus einem der zugehörigen Protokollspeicher lesen kann. Rohereignisse für das Betriebssystem, andere Datenbanken und verschiedene Sicherheitsanwendungen werden separat für die Ereignisquelle gespeichert.

Ereignisse

Ereignisse in CA Enterprise Log Manager sind Protokolldatensätze, die von jeder angegebenen Ereignisquelle generiert werden.

Ereignisverfeinerung

Ereignisverfeinerung bezeichnet den Prozess, in dem die Zeichenfolge eines erfassten Rohereignisses in die jeweiligen Ereignisfelder und die zugeordneten CEG-Felder analysiert wird. Benutzer können Abfragen durchführen, um die Ergebnisse der verfeinerten Ereignisdaten anzuzeigen. Die Ereignisverfeinerung findet nach der Ereigniserfassung und vor der Ereignisspeicherung statt.

Ereignisverfeinerungs-Bibliothek

Die *Ereignisverfeinerungs-Bibliothek* ist der Speicher für vordefinierte und benutzerdefinierte Integrationen, für Zuordnungs- und Analysedateien sowie für Unterdrückungs- und Zusammenfassungsregeln.

Ereignisweiterleitungsregeln

Ereignisweiterleitungsregeln geben an, dass ausgewählte Ereignisse nach der Speicherung im Ereignisprotokoll-Speicher an Produkte anderer Hersteller weitergeleitet werden sollen, beispielsweise an Produkte zur Korrelation von Ereignissen.

Erfassungspunkt

Ein *Erfassungspunkt* ist ein Server, auf dem ein Agent installiert ist und bei dem sich der Server in unmittelbarer Netzwerknähe zu allen Servern mit Ereignisquellen befindet, die mit den Connectors des Agenten verknüpft sind.

Erfassungsserver

Ein *Erfassungsserver* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Ein Erfassungsserver verfeinert eingehende Ereignisprotokolle, fügt sie in die heiße Datenbank ein, komprimiert die heiße Datenbank und archiviert oder kopiert sie automatisch auf den entsprechenden Berichtsserver. Der Erfassungsserver komprimiert die heiße Datenbank, sobald diese die konfigurierte Größe erreicht hat, und archiviert sie automatisch entsprechend dem konfigurierten Plan.

Filter

Ein *Filter* ist ein Mittel, mit dem Sie eine Abfrage für den Ereignisprotokollspeicher eingrenzen können.

Föderationsserver

Föderationsserver sind CA Enterprise Log Manager-Server, die in einem Netzwerk miteinander verbunden sind, um die erfassten Protokolldaten zu verteilen, aber um die erfassten Daten für die Berichterstellung zu aggregieren. Föderationsserver können hierarchisch oder über eine vernetzte Topologie verbunden werden. Berichte von föderierten Daten umfassen Daten vom Zielserver sowie Daten von Unter- oder Gleichordnungen dieses Servers, sofern vorhanden.

Funktionszuordnungen

Funktionszuordnungen sind ein optionaler Teil der Datenzuordnungsdatei für eine Produktintegration. Mit einer Funktionszuordnung kann ein CEG-Feld gefüllt werden, wenn der benötigte Wert nicht direkt vom Quellereignis abgerufen werden kann. Alle Funktionszuordnungen bestehen aus dem Namen des CEG-Feldes, einem vordefinierten oder Klassenfeldwert und der Funktion, mit der der Wert abgerufen oder berechnet wird.

Gespeicherte Konfiguration

Eine *gespeicherte Konfiguration* ist eine gespeicherte Konfiguration mit den Werten für die Datenzugriffsattribute einer Integration, die als Vorlage bei der Erstellung einer neuen Integration verwendet werden kann.

Globale Gruppe

Eine *globale Gruppe* ist eine Gruppe, die von mehreren Anwendungsinstanzen gemeinsam verwendet wird, die im selben CA Enterprise Log Manager-Management-Server registriert sind. Jeder Benutzer kann einer oder mehreren globalen Gruppen zugeordnet werden. Zugriffsrichtlinien können mit globalen Gruppen als Identitäten definiert werden, denen die Durchführung bestimmter Aktionen in ausgewählten Ressourcen gewährt oder verweigert wird.

Globale Konfiguration

Die *global Konfiguration* bezeichnet eine Reihe von Einstellungen, die alle CA Enterprise Log Manager-Server betreffen, die denselben Management-Server verwenden.

Globale Ressource

Eine *globale Ressource* für das CA Enterprise Log Manager-Produkt ist eine Ressource, die mit anderen CA-Anwendungen gemeinsam genutzt wird. Sie können Richtlinien zur Bereichsdefinierung mit globalen Ressourcen erstellen. Beispiele hierfür sind Benutzer, Richtlinien und Kalender. Siehe auch Anwendungsressource.

Globaler Benutzer

Bei einem *globalen Benutzer* handelt es sich um die Benutzerkontoinformationen ohne anwendungsspezifische Details. Die Details und eines globalen Benutzers und die Mitgliedschaften einer globalen Gruppe werden gemeinsam in allen CA-Anwendungen genutzt, die mit dem Standardbenutzerspeicher integriert werden können. Die Details globaler Benutzer können im eingebetteten Repository oder in einem externen Verzeichnis gespeichert werden.

Globaler Filter

Ein *globaler Filter* ist ein Satz von Kriterien, die Sie angeben können und mit denen die in den Berichten angezeigten Daten begrenzt werden können. Beispielsweise zeigt ein globaler Filter für die letzten 7 Tage nur die Ereignisse an, die in den letzten sieben Tagen generiert wurden.

Hierarchische Föderation

Eine *hierarchische Föderation* von CA Enterprise Log Manager-Servern ist eine Topologie, die eine hierarchische Beziehung zwischen Servern einrichtet. In seiner einfachsten Form ist dies der Fall, wenn Server 2 ein untergeordneter Server von Server 1 ist, Server 1 jedoch nicht Server 2 untergeordnet ist. Dies bedeutet, dass die Beziehung nur in eine Richtung geht. Eine hierarchische Föderation kann mehrere Ebenen von über- und untergeordneten Beziehungen haben, und ein einzelner übergeordneter Server kann mehrere untergeordnete Server haben. Eine föderierte Abfrage gibt die Ergebnisse vom ausgewählten Server und all seinen untergeordneten Servern zurück.

Hilfsprogramm "LMArchive"

Das *Hilfsprogramm "LMArchive"* ist das Befehlszeilenhilfsprogramm, mit dem die Sicherung und Wiederherstellung von Archivdatenbanken zum Ereignisprotokollspeicher auf einem CA Enterprise Log Manager-Server verfolgt wird. Mit "LMArchive" können Sie die Liste der warmen Datenbankdateien abfragen, die für die Archivierung bereit sind. Nach der Sicherung der aufgelisteten Datenbank und nach deren Verschieben in den langfristigen (kalten) Speicher können Sie mit "LMArchive" einen Datensatz im CA Enterprise Log Manager erstellen, dass diese Datenbank gesichert wurde. Nach der Wiederherstellung einer kalten Datenbank in ihrem ursprünglichen CA Enterprise Log Manager können Sie mit "LMArchive" CA Enterprise Log Manager benachrichtigen, der dann die Datenbankdateien wiederum verfügbar macht, so dass sie abgefragt werden können.

Hilfsprogramm "LMSEOSImport"

Das Hilfsprogramm *LMSEOSImport* ist ein Befehlszeilenhilfsprogramm, mit dem SEOSDATA oder vorhandene Ereignisse als Teil der Migration von Audit Reporter, Viewer oder Audit Collector in CA Enterprise Log Manager importiert werden. Dieses Hilfsprogramm wird nur von Microsoft Windows und Sun Solaris Sparc unterstützt.

Hilfsprogramm "scp"

Die Sicherheitskopie *scp* (Kopierprogramm für Remote-Dateien) ist ein UNIX-Hilfsprogramm, das Dateien zwischen UNIX-Computern in einem Netzwerk transferiert. Dieses Hilfsprogramm wird während der CA Enterprise Log Manager-Installation für Sie zur Verfügung gestellt, damit Sie Dateien für automatische Software-Updates vom Online-Proxy zum Offline-Proxy für Software-Updates transferieren können.

HTTP-Proxy-Server

Ein *HTTP-Proxy-Server* ist ein Proxy-Server, der wie eine Firewall agiert und dafür sorgt, dass Internet-Traffic das Unternehmen nur über den Proxy betritt und wieder verlässt. Wenn bei ausgehendem Verkehr eine ID und ein Kennwort angegeben werden, kann der Proxy-Server umgangen werden. Beim Verwalten automatischer Software-Updates kann die Verwendung eines lokalen HTTP-Proxy-Servers konfiguriert werden.

Idealmodell (ideal_model)

Das *Idealmodell* stellt die Technologie dar, die das Ereignis ausdrückt. Dies ist das erste CEG-Feld in einer Hierarchie von Feldern, die für die Ereignisklassifikation und -normalisierung verwendet werden. Beispiele eines Idealmodells sind z. B. Antivirus, DBMS, Firewall, Betriebssystem und Webserver. Die Firewall-Produkte Check Point, Cisco PIX und Netscreen/Juniper könnten mit dem Wert "Firewall" im Feld "ideal_model" normalisiert werden.

Identität

Eine *Identität* in CA Enterprise Log Manager ist eine Benutzergruppe, die Zugriff auf die CAELM-Anwendungsinstanz und ihre Ressourcen hat. Eine Identität für ein CA-Produkt kann ein globaler Benutzer, ein Anwendungsbenutzer, eine globale Gruppe, eine Anwendungsgruppe oder eine dynamische Gruppe sein.

Inhaltsaktualisierungen

Inhaltsaktualisierungen sind der nicht-binäre Anteil der automatischen Software-Updates, die auf dem CA Enterprise Log Manager-Management-Server gespeichert werden. Inhaltsaktualisierungen umfassen Inhalte, wie XMP-Dateien, Datenzuordnungsdateien, Konfigurationsaktualisierungen für CA Enterprise Log Manager-Module und Aktualisierungen öffentlicher Schlüssel.

Installierender

Der *Installierende* ist derjenige, der die Soft-Appliance und die Agenten installiert. Während des Installationsprozesses werden die Benutzernamen "caelmadmin" und "EiamAdmin" erstellt, und das für "EiamAdmin" angegebene Kennwort wird "caelmadmin" zugewiesen. Diese "caelmadmin"-Anmeldeinformationen werden für den ersten Zugriff auf das Betriebssystem benötigt, die "EiamAdmin"-Anmeldeinformationen werden für den ersten Zugriff auf die CA Enterprise Log Manager-Software und für die Installation der Agenten benötigt.

Integration

Integration ist das Mittel, mit dem nicht klassifizierte Ereignisse in verfeinerte Ereignisse verarbeitet werden, so dass sie in Abfragen und Berichten angezeigt werden. Die Integration wird mit einem Satz von Elementen implementiert, die es einem bestimmten Agenten und Connector ermöglichen, Ereignisse von einem oder mehreren Typen von Ereignisquellen zu erfassen und zu CA Enterprise Log Manager zu senden. Der Satz von Elementen umfasst den Protokollsensor und die XMP- und DM-Dateien, die aus einem bestimmten Produkt lesen sollen. Beispiele für vordefinierte Integrationen sind die für die Verarbeitung von Syslog- und WMI-Ereignissen. Sie können benutzerdefinierte Integrationen erstellen, um die Verarbeitung nicht klassifizierter Ereignisse zu ermöglichen.

Integrationselemente

Integrationselemente umfassen einen Sensor, eine Konfigurationshilfe, eine Datenzugriffsdatei, eine oder mehrere XMP-Nachrichtenanalysedateien und eine oder mehrere Datenzuordnungsdateien.

iTech-Ereignis-Plugin

Das *iTech-Ereignis-Plugin* ist ein CA-Adapter, den ein Administrator mit ausgewählten Zuordnungsdateien konfigurieren kann. Er erhält Ereignisse von Remote-iRecorders, CA EEM, iTechnology selbst oder von einem Produkt, das Ereignisse über iTechnology sendet.

Kalender

Ein *Kalender* ist ein Mittel, mit dem Sie die Gültigkeitsdauer einer Zugriffsrichtlinie begrenzen können. Eine Richtlinie ermöglicht bestimmten Identitäten die Durchführung bestimmter Aktionen in einer angegebenen Ressource während eines definierten Zeitraums.

Katalog

Der *Katalog* ist die Datenbank auf jedem CA Enterprise Log Manager, die den Status der archivierten Datenbanken beibehält und gleichzeitig als Index höchster Ebene für alle Datenbanken agiert. Die Statusinformationen (warm, kalt oder verfügbar gemacht) werden für alle Datenbanken beibehalten, die sich je auf diesem CA Enterprise Log Manager befunden haben, und für jede Datenbank, die auf diesem CA Enterprise Log Manager als verfügbar gemachte Datenbank wiederhergestellt wurde. Die Indizierungsfähigkeit erstreckt sich auf alle heißen und warmen Datenbanken im Ereignisprotokollspeicher auf diesem CA Enterprise Log Manager.

Kennung

Eine *Kennung* ist ein Term oder eine Schlüsselphrase, mit der Abfragen oder Berichte identifiziert werden, die zur selben geschäftsrelevanten Gruppierung gehören. Kennungen ermöglichen Suchläufe, die auf geschäftsrelevanten Gruppierungen basieren. Eine Kennung ist außerdem der Ressourcenname, der in einer Richtlinie verwendet wird, die dem Benutzer die Berechtigung zur Erstellung einer Kennung erteilt.

Konto

Ein *Konto* bezeichnet einen globalen Benutzer, der auch ein CALM-Anwendungsbenutzer ist. Eine einzelne Person kann mehr als ein Konto haben, jedoch muss die benutzerdefinierte Rolle eine andere sein.

Lokaler Filter

Ein *lokaler Filter* ist ein Satz von Kriterien, die Sie während der Berichtsanzeige angeben können, um die angezeigten Daten für den aktuellen Bericht zu begrenzen.

Lokales Ereignis

Ein *lokales Ereignis* ist ein Ereignis, das eine einzelne Einheit umfasst, bei der sich Quelle und Ziel des Ereignisses auf demselben Hostrechner befinden. Ein lokales Ereignis entspricht Typ 1 der vier Ereignistypen, die in der ELM-Schemadefinition (CEG) verwendet werden.

Management-Server

Der *Management-Server* ist eine Rolle, die dem ersten installierten CA Enterprise Log Manager-Server zugewiesen ist. Dieser CA Enterprise Log Manager-Server enthält das Repository, in dem gemeinsam genutzte Inhalte, wie Richtlinien, für all seine CA Enterprise Log Managers gespeichert werden. Dieser Server ist normalerweise der Standard-Proxy für automatische Software-Updates. Auch wenn dies in den meisten produktiven Umgebungen nicht empfehlenswert ist, so kann der Management-Server alle Rollen ausführen.

MIB (Management Information Base)

Die *MIB (Management Information Base)* für CA Enterprise Log Manager, CA-ELM.MIB, muss für jedes Produkt, das Alarme in Form von SNMP-Traps von CA Enterprise Log Manager erfassen soll, importiert und konfiguriert werden. Die MIB zeigt die Quelle der numerischen OIDs (Objekt-ID) an, die in einer SNMP-Trap-Meldung verwendet werden, zusammen mit einer Beschreibung des Datenobjekts oder Netzwerkelements. In der MIB für SNMP-Traps, die von CA Enterprise Log Manager gesendet werden, bezieht sich die Beschreibung der einzelnen Datenobjekte auf das entsprechende CEG-Feld. Die MIB stellt sicher, dass alle Namen-/Wertepaare aus einer SNMP-Trap am Ziel korrekt interpretiert werden.

Modul für automatische Software-Updates

Das *Modul für automatische Software-Updates* ist ein Dienst, bei dem automatische Software-Updates über den CA-Software-Update-Server automatisch heruntergeladen und an CA Enterprise Log Manager-Server und an alle Agenten verteilt werden können. Globale Einstellungen gelten für lokale CA Enterprise Log Manager-Server. Lokale Einstellungen geben an, ob der Server ein Offline-Proxy, ein Online-Proxy oder ein Client für automatische Software-Updates ist.

Module (zum Herunterladen)

Ein *Modul* ist eine logische Gruppierung von Komponentenaktualisierungen, die über ein automatisches Software-Update zum Herunterladen zur Verfügung gestellt wird. Ein Modul kann binäre Aktualisierungen, Inhaltsaktualisierungen oder beides enthalten. Beispielsweise bilden alle Berichte ein Modul und alle Sponsor-Binäraktualisierungen ein anderes. CA definiert, was ein Modul ausmacht.

Nachrichtenanalyse

Nachrichtenanalyse bezeichnet die Anwendung von Regeln auf die Analyse eines Rohereignisprotokolls, um relevante Informationen (wie Zeitstempel, IP-Adresse und Benutzername) abzurufen. Analyseregeln arbeiten mit der Zeichenübereinstimmung, um einen bestimmten Ereignistext zu suchen und diesen mit den ausgewählten Werten zu verknüpfen.

Nachrichtenanalyse

Die *Analyse*, auch als Nachrichtenanalyse bezeichnet, umfasst den Prozess der Umwandlung roher Gerätedaten in Schlüsselwertpaare. Die Nachrichtenanalyse wird durch eine XMP-Datei gesteuert. Die Analyse, die der Datenzuordnung vorausgeht, ist ein Schritt des Integrationsprozesses, der das von einer Ereignisquelle erfasste Rohereignis in ein verfeinertes Ereignis umwandelt, das Sie anzeigen können.

Nachrichtenanalysebibliothek

Die *Nachrichtenanalysebibliothek* ist eine Bibliothek, die Ereignisse aus den Listener-Warteschlangen übernimmt und reguläre Ausdrücke verwendet, um Zeichenfolgen in Token-Namenwertpaare zu übersetzen.

Nachrichtenanalysedatei (XMP)

Eine *Nachrichtenanalysedatei (XMP)* ist eine XML-Datei, die mit einem bestimmten Ereignisquellentyp verknüpft ist, der Analyseregeln anwendet. Analyseregeln zerlegen die relevanten Daten in einem erfassten Rohereignis in Namenswertepaare, die dann zur weiteren Verarbeitung an die Datenzuordnungsdatei weitergeleitet werden. Dieser Dateityp wird in allen Integrationen sowie in Connectors verwendet, die auf Integrationen basieren. Im Falle von CA-Adaptern können XMP-Dateien auch auf dem CA Enterprise Log Manager-Server angewendet werden.

Nachrichtenanalyse-Token (ELM)

Ein *Nachrichtenanalyse-Token* ist eine wiederverwendbare Vorlage für die Erstellung einer regulären Ausdruckssyntax, die bei der CA Enterprise Log Manager-Nachrichtenanalyse verwendet wird. Ein Token verfügt über einen Namen, einen Typ und eine entsprechende Zeichenfolge für den regulären Ausdruck.

Natives Ereignis

Ein *natives Ereignis* ist der Zustand oder die Aktion, die ein Rohereignis auslöst. Native Ereignisse werden empfangen, entsprechend analysiert/zugeordnet und dann als Rohereignisse oder verfeinerte Ereignisse übertragen. Eine fehlgeschlagene Authentifizierung ist ein natives Ereignis.

Neukatalogisierung

Eine *Neukatalogisierung* ist eine erzwungene Neuerstellung des Katalogs. Die Neukatalogisierung ist nur erforderlich, wenn Daten im Ereignisprotokollspeicher eines anderen Servers wiederhergestellt werden als auf dem Server, auf dem sie generiert wurden. Wenn Sie einen CA Enterprise Log Manager als Wiederherstellungspunkt für Untersuchungen von kalten Daten bestimmen, müssen Sie eine Neukatalogisierung der Datenbank immer dann erzwingen, nachdem diese auf dem festgelegten Wiederherstellungspunkt wiederhergestellt wurde. Eine Neukatalogisierung wird ggf. automatisch durchgeführt, wenn iGateway erneut gestartet wird. Die Neukatalogisierung einer einzelnen Datenbank kann mehrere Stunden in Anspruch nehmen.

NIST

Das *National Institute of Standards and Technology (NIST)* ist die Bundesagentur, die Empfehlungen in ihrer Special Publication 800-92 *Guide to Computer Security Log Management* (Leitfaden für die Computersicherheitsprotokoll-Verwaltung) gibt, die als Basis für CA Enterprise Log Manager verwendet wurde.

ODBC- und JDBC-Zugriff

Durch den *ODBC- und JDBC-Zugriff* auf CA Enterprise Log Manager-Ereignisprotokoll-Speicher wird die Verwendung von Ereignisdaten mit einer Vielzahl von Produkten anderer Hersteller unterstützt, darunter die benutzerdefinierte Berichterstellung zu Ereignissen mit Berichterstellungstools anderer Hersteller, die Ereigniskorrelation mit Korrellations-Engines und die Ereignisauswertung durch Produkte für die Erkennung von Sicherheitsverletzungen (Intrusion Detection) und Malware. Auf Systemen mit Windows-Betriebssystemen wird der ODBC-Zugriff verwendet, auf UNIX- und Linux-Systemen hingegen der JDBC-Zugriff.

ODBC-Server

Der *ODBC-Server* ist der konfigurierte Service, der den für die Kommunikation zwischen dem ODBC- oder JDBC-Client und dem CA Enterprise Log Manager-Server verwendeten Port festlegt und angibt, ob SSL-Verschlüsselung verwendet werden soll.

OID (Objekt-ID)

Eine *OID (Objekt-ID)* ist eine eindeutige numerische ID für ein Datenobjekt, das mit Werten in einer SNMP-Trap-Meldung verbunden wird. Alle OIDs, die in einer CA Enterprise Log Manager-SNMP-Trap verwendet werden, werden einem CEG-Textfeld in der MIB zugeordnet. Jede OID, die einem CEG-Feld zugeordnet ist, hat folgende Syntax: 1.3.6.1.4.1.791.9845.x.x.x, wobei 791 die Unternehmensnummer für CA und 9845 die Produkt-ID für CA Enterprise Log Manager ist.

Ordner

Ein *Ordner* ist ein Verzeichnispfad-Speicherort, an dem der CA Enterprise Log Manager-Management-Server die CA Enterprise Log Manager-Objekttypen speichert. Sie sollten Ordner in Richtlinien zur Bereichsdefinierung referenzieren, um Benutzern die Berechtigung zum Zugriff auf einen bestimmten Objekttyp zu erteilen oder zu verweigern.

Pflichtrichtlinie

Eine *Pflichtrichtlinie* ist eine Richtlinie, die beim Erstellen eines Zugriffsfilters automatisch erstellt wird. Sie sollten nicht versuchen, eine Pflichtrichtlinie direkt zu erstellen, zu bearbeiten oder zu löschen. Erstellen, bearbeiten oder löschen Sie stattdessen den Zugriffsfilter.

pozFolder

Der *pozFolder* ist ein Attribut des Anwendungsobjekts, wobei der Wert dem übergeordneten Pfad des Anwendungsobjekt entspricht. Attribut und Wert von "pozFolder" werden in Filtern für Zugriffsrichtlinien verwendet, die den Zugriff auf Ressourcen wie Berichte, Abfragen und Konfigurationen einschränken.

Profil

Ein *Profil* ist ein optionaler, konfigurierbarer Satz von Kennungs- und Datenfiltern, die produktspezifisch, technologiespezifisch oder auf eine ausgewählte Kategorie beschränkt sind. Ein Kennungsfilter für ein Produkt beschränkt beispielsweise die gelisteten Kennungen auf die ausgewählte Produktkennung. Datenfilter für ein Produkt zeigen in den von Ihnen generierten Berichten, den von Ihnen geplanten Alarmen und den von Ihnen angezeigten Abfrageergebnissen nur die Daten für das angegebene Produkt an. Nachdem Sie das gewünschte Profil erstellt haben, können Sie es, sobald Sie angemeldet sind, jederzeit aktivieren. Wenn Sie mehrere Profile erstellen, können Sie in einer Sitzung verschiedene Profile, jeweils eins nach dem anderen auf Ihre Aktivitäten anwenden. Vordefinierte Filter erhalten Sie mit den automatischen Software-Updates.

Protokoll

Ein *Protokoll* ist ein Audit-Datensatz oder eine erfasste Nachricht eines Ereignisses oder mehrerer Ereignisse. Ein Protokoll kann ein Audit-Protokoll, ein Transaktionsprotokoll, ein Intrusionsprotokoll, ein Verbindungsprotokoll, ein Systemleistungsdatensatz, ein Benutzeraktivitätsprotokoll oder ein Alarm sein.

Protokollanalyse

Protokollanalyse ist eine Untersuchung der Protokolleinträge, um relevante Ereignisse festzustellen. Wenn Protokolle nicht zeitnah analysiert werden, verringert sich ihr Wert beträchtlich.

Protokollanalyse

Protokollanalyse ist der Prozess der Datenextraktion aus einem Protokoll, damit die analysierten Werte in einem Folgestadium der Protokollverwaltung verwendet werden können.

Protokollarchivierung

Protokollarchivierung bezeichnet den Prozess, der auftritt, wenn die heiße Datenbank ihre Maximalgröße erreicht, wenn eine Komprimierung auf Zeilenebene durchgeführt wird und der Status von heiß in warm geändert wird. Administratoren müssen die warme Datenbank sichern, bevor die Schwelle zum Löschen erreicht wird, und sie müssen das Hilfsprogramm "LMArchive" ausführen, um den Namen der Sicherungen zu erfassen. Diese Informationen stehen dann zur Anzeige über die Archivabfrage zur Verfügung.

Protokolldatensatz

Ein *Protokolldatensatz* ist ein einzelner Audit-Datensatz.

Protokolleintrag

Ein *Protokolleintrag* ist ein Eintrag in einem Protokoll, der Informationen zu einem bestimmten Ereignis enthält, das in einem System oder Netzwerk aufgetreten ist.

Protokollsensor

Ein *Protokollsensor* ist eine Integrationskomponente, die Daten aus einem bestimmten Typ lesen soll, wie z. B. aus Datenbank, Syslog, Datei oder SNMP. Protokollsensoren werden wiederverwendet. Normalerweise erstellen die Benutzer keine benutzerdefinierten Protokollsensoren.

Proxy für automatische Software-Updates (offline)

Ein *Offline-Proxy für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server, der automatische Software-Updates über eine manuelle Verzeichniskopie (unter Verwendung von scp) von einem Online-Proxy für automatische Software-Updates erhält. Offline-Proxys für automatische Software-Updates können so konfiguriert werden, dass Sie binäre Updates zu Clients herunterladen, die diese anfordern, und dass sie die aktuellste Version der Inhaltsaktualisierungen an den Management-Server weiterleiten, wenn dieser sie noch nicht erhalten hat. Offline-Proxys für automatische Software-Updates benötigen keinen Internetzugang.

Proxy für automatische Software-Updates (online)

Ein *Online-Proxy für automatische Software-Updates* ist ein CA Enterprise Log Manager-Server mit Internetzugang, der automatische Software-Updates nach einem wiederkehrenden Zeitplan von einem CA-Server für automatische Software-Updates erhält. Ein bestimmter Online-Proxy für automatische Software-Updates kann für einen oder mehrere Clients in die Proxy-List aufgenommen werden. Dieser kontaktiert die aufgelisteten Proxys im Ringversuch, um binäre Aktualisierungen anzufordern. Ein bestimmter Online-Proxy leitet, wenn er so konfiguriert wurde, neue Inhalts- und Konfigurationsaktualisierungen an den Management-Server weiter, wenn diese nicht bereits von einem anderen Proxy weitergeleitet wurden. Das Verzeichnis für automatische Software-Updates eines ausgewählten Online-Proxys wird beim Kopieren von Aktualisierungen in Offline-Proxys automatischer Software-Updates als Quelle verwendet.

Proxy für automatische Software-Updates (Standardwert)

Der *Standard-Proxy für automatische Software-Updates* ist normalerweise der CA Enterprise Log Manager-Server, der als erster installiert wurde und der auch der primäre CA Enterprise Log Manager sein kann. Der Standard-Proxy für automatische Software-Updates ist außerdem ein Online-Proxy für automatische Software-Updates und muss daher über einen Internetzugang verfügen. Wenn keine anderen Online-Proxys für automatische Software-Updates definiert werden, erhält dieser Server die automatischen Software-Updates vom CA-Server für automatische Software-Updates, lädt die Binäraktualisierungen an alle Clients herunter und leitet die Inhaltsaktualisierungen an CA EEM weiter. Wenn andere Proxys definiert sind, erhält dieser Server die automatischen Software-Updates immer noch, aber er wird von Clients nur dann wegen Aktualisierungen kontaktiert, wenn keine Proxy-Liste für automatische Software-Updates konfiguriert wurde bzw. wenn die konfigurierte Liste erschöpft ist.

Proxys für Software-Updates (für Client)

Die *Proxys für Software-Updates für den Client* bilden die Proxy-Liste für automatische Software-Updates, die der Client in einem Ringversuch kontaktiert, um die CA Enterprise Log Manager-Software- und die Betriebssystem-Software-Updates abzurufen. Wenn ein Proxy beschäftigt ist, wird der nächste in der Liste kontaktiert. Wenn keiner zur Verfügung steht und der Client online ist, wird der Standard-Proxy für Software-Updates verwendet.

Proxys für Software-Updates (für Inhaltsaktualisierungen)

Proxys für Software-Updates (für Inhaltsaktualisierungen) sind die Proxys, die für die Aktualisierung des CA Enterprise Log Manager-Management-Servers mit Inhaltsaktualisierungen ausgewählt wurden, die vom CA-Server für automatische Software-Updates heruntergeladen werden. Ein bewährtes Verfahren ist die Konfiguration mehrerer Proxys aus Gründen der Redundanz.

Prozess mit dynamischen Werten

Ein *Prozess mit dynamischen Werten* ist ein CA IT PAM-Prozess, den Sie aufrufen, um die Werteliste für einen in Berichten oder Alarmen verwendeten, ausgewählten Schlüssel aufzufüllen oder zu aktualisieren. Sie stellen den Pfad zum Prozess mit dynamischen Werten als Teil der IT PAM-Konfiguration für die Service-Liste des Berichtsservers auf der Registerkarte "Verwaltung" bereit. Im Abschnitt "Werte", der mit den Schlüsselwerten auf derselben Seite der Benutzeroberfläche verknüpft ist, klicken Sie auf "Liste der dynamischen Werte importieren". Das Aufrufen des Prozesses mit dynamischen Werten ist eine von drei Möglichkeiten, wie Sie den Schlüsseln Werte hinzufügen können.

Remote-Ereignis

Ein *Remote-Ereignis* ist ein Ereignis, das zwei verschiedene Hostrechner umfasst, die Quelle und das Ziel. Ein Remote-Ereignis entspricht Typ 2 der vier Ereignistypen, die in der ELM-Schemadefinition (CEG) verwendet werden.

Remote-Speicher-Server

Ein *Remote-Speicher-Server* ist eine Rolle, die einem Server zugewiesen wird, der automatisch archivierte Datenbanken von einem oder mehreren Berichtsservern empfängt. In einem Remote-Speicher-Server können kalte Datenbanken für die benötigte Anzahl an Jahren gespeichert werden. Auf dem Remote-Host, der zum Speichern verwendet wird, sind normalerweise kein CA Enterprise Log Manager oder andere Produkte installiert. Konfigurieren Sie für die Auto-Archivierung eine nicht-interaktive Authentifizierung.

Richtlinie zur Bereichsdefinierung

Eine *Richtlinie zur Bereichsdefinierung* ist ein Typ einer Zugriffsrichtlinie, die den Zugriff auf Ressourcen, die auf dem Management-Server gespeichert sind, (wie z. B. Anwendungsobjekte, Benutzer, Gruppen, Ordner und Richtlinien) gewährt oder verweigert. Mit der Richtlinie zur Bereichsdefinierung werden die Identitäten festgelegt, die auf die angegebenen Ressourcen zugreifen dürfen.

Rohereignis

Ein *Rohereignis* stellt die Informationen dar, die von einem nativen Ereignis ausgelöst werden, das von einem Überwachungsagenten zum Protokollmanager-Collector gesendet wird. Das Rohereignis wird häufig als Syslog-Zeichenfolge oder als Namenswertpaare formatiert. Es ist möglich, ein Ereignis in seiner Rohform in CA Enterprise Log Manager anzuzeigen.

RSS-Ereignis

Ein *RSS-Ereignis* ist ein Ereignis, das von CA Enterprise Log Manager generiert wird, um einen Aktionsalarm an Drittanbieterprodukte und -benutzer zu leiten. Das Ereignis besteht aus einer Zusammenfassung aller Aktionsalarmergebnisse und einem Link zur Ergebnisdatei. Die Dauer eines bestimmten RSS-Feed-Elements ist konfigurierbar.

RSS-Feed-URL für Aktionsalarme

Die *RSS-Feed-URL für Aktionsalarme* lautet: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. Von dieser URL können Sie das maximale Alter sowie die maximale Menge für Aktionsalarme anzeigen, die zu dieser Konfiguration gehören.

RSS-Feed-URL für Software-Updates

Die *RSS-Feed-URL für Software-Updates* ist ein vorkonfigurierter Link, der von Online-Proxy-Servern für Software-Updates bei der Abfrage von automatischen Software-Updates verwendet wird. Diese URL ist für den CA-Server für automatische Software-Updates bestimmt.

SafeObject

SafeObject ist eine vordefinierte Ressourcenklasse in CA EEM. Es ist die Ressourcenklasse, zu der Anwendungsobjekte, die im Bereich der Anwendung gespeichert sind, gehören. Benutzer, die Richtlinien und Filter für die Erteilung des Zugriffs auf Anwendungsobjekte definieren, beziehen sich auf diese Ressourcenklasse.

SAPI-Collector

Der *SAPI-Collector* ist ein CA-Adapter, der Ereignisse von CA Audit-Clients erhält. CA Audit-Clients senden mit der Aktion "Collector", die über einen integrierten Failover verfügt. Administratoren konfigurieren den CA Audit-SAPI-Collector beispielsweise mit ausgewähltem Chiffre und Datenzuordnungsdateien.

SAPI-Recorder

Ein *SAPI-Recorder* bezeichnet die Technologie, die vor iTechnology zum Versenden von Informationen an CA Audit verwendet wurde. SAPI steht für Submit Application Programming Interface (API starten). CA Audit-Recorder für CA ACF2, CA Top Secret, RACF, Oracle, Sybase und DB2 sind Beispiele für SAPI-Recorder.

SAPI-Router

Der *SAPI-Router* ist ein CA-Adapter, der Ereignisse aus Integrationen erhält, wie z. B. Mainframe, und diese an einen CA Audit-Router.

Schlüsselwerte

Schlüsselwerte sind benutzerdefinierte Werte, die einer benutzerdefinierten Liste (Schlüsselgruppe) zugewiesen werden. Wenn eine Abfrage eine Schlüsselgruppe verwendet, enthalten die Suchergebnisse Übereinstimmungen mit beliebigen Schlüsselwerten in der Schlüsselgruppe. Es gibt mehrere vordefinierte Schlüsselgruppen, einige von diesen enthalten vordefinierte Schlüsselwerte, die in vordefinierten Abfragen und Berichten verwendet werden.

Selbstüberwachendes Ereignis

Ein *selbstüberwachendes Ereignis* ist ein Ereignis, das von CA Enterprise Log Manager protokolliert wird. Solche Ereignisse werden automatisch durch Aktionen generiert, die von angemeldeten Benutzern und Funktionen durchgeführt wurden, die wiederum von verschiedenen Modulen wie den Services oder Listeners ausgeführt wurden. Der Bericht für SIM-Operationen/selbstüberwachende Ereignisdetails kann angezeigt werden, indem Sie einen Berichtsserver auswählen und die Registerkarte "Selbstüberwachende Ereignisse" öffnen.

Services

Die CA Enterprise Log Manager-*Services* sind Ereignisprotokollspeicher, Berichtsserver und automatisches Software-Update. Administratoren konfigurieren diese Services auf einer globalen Ebene, bei der standardmäßig alle Einstellungen auf alle CA Enterprise Log Managers angewendet werden. Die meisten globalen Einstellungen für Services können auf der lokalen Ebene, also für jeden angegebenen CA Enterprise Log Manager, überschrieben werden.

SNMP

SNMP ist ein Akronym und steht für "Simple Network Management Protocol", einen offenen Standard zum Senden von Warnmeldungen in Form von SNMP-Traps von einem Agentensystem an mehrere Managementsysteme.

SNMP-Trap-Inhalte

Eine *SNMP-Trap* besteht aus Namen-/Wertepaaren, wobei jeder Name eine OID (Objekt-ID) und jeder Wert ein zurückgegebener Wert aus dem geplanten Alarm ist. Abfrageergebnisse, die von einem Aktionsalarm zurückgegeben werden, bestehen aus CEG-Feldern und ihren Werten. SNMP-Traps werden ausgefüllt, indem die CEG-Felder der Namen in den Namen-/Wertepaaren durch OIDs ersetzt werden. Die Zuordnung zwischen CEG-Feld und OID wird in der MIB gespeichert. Die SNMP-Trap enthält nur Namen-/Wertepaare für Felder, die Sie beim Konfigurieren des Alarms ausgewählt haben.

SNMP-Trap-Ziele

Beim Planen von Aktionsalarmen können ein oder mehrere *SNMP-Trap-Ziele* hinzugefügt werden. Für jedes SNMP-Trap-Ziel wird eine IP-Adresse und eine Port konfiguriert. Das Ziel ist typischerweise ein NOC oder ein Verwaltungsserver, z. B. CA Spectrum oder CA NSM. Eine SNMP-Trap wird an die konfigurierten Ziele gesendet, wenn Abfragen für einen geplanten Alarmjob Ergebnisse zurückgeben.

Soft-Appliance

Die *Soft-Appliance* umfasst eine Betriebssystemkomponente und die CA Enterprise Log Manager-Software-Komponente.

Standardagent

Der *Standardagent* ist der integrierte Agent, der mit dem CA Enterprise Log Manager-Server installiert wird. Er kann für die direkte Erfassung von Syslog-Ereignissen sowie von Ereignissen von verschiedenen Nicht-Syslog-Ereignisquellen wie CA Access Control r12 SP1, Microsoft Active Directory-Zertifikatdiensten und Oracle9i-Datenbanken konfiguriert werden.

Unterdrückung

Unterdrückung ist der Prozess, in dem Ereignisse auf der Basis von CEG-Filtern verworfen werden. Die Unterdrückung wird durch eine SUP-Datei gesteuert.

Unterdrückungsregeln

Unterdrückungsregeln sind Regeln, die Sie konfigurieren, um zu verhindern, dass bestimmte verfeinerte Ereignisse in Ihren Berichten angezeigt werden. Sie können permanente Unterdrückungsregeln erstellen, um nicht sicherheitsrelevante Routineereignisse zu unterdrücken. Sie können aber auch temporäre Regeln erstellen, um die Protokollierung geplanter Ereignisse, wie die Erstellung vieler neuer Benutzer, zu unterdrücken.

URL für CA Embedded Entitlements Manager

Die *URL für CA Embedded Entitlements Manager* (CA EEM) lautet: https://<ip_address>:5250/spin/eiam. Um sich anzumelden, wählen Sie "CAELM" als die Anwendung und geben das Kennwort ein, das mit dem Benutzernamen "EiamAdmin" verknüpft ist.

URL für CA Enterprise Log Manager

Die *URL für CA Enterprise Log Manager* lautet: https://<ip_address>:5250/spin/calm. Um sich anzumelden, geben Sie den Benutzernamen, der vom Administrator für dieses Konto definiert wurde, sowie den zugehörige Kennwort ein. Oder Sie geben "EiamAdmin", den Standardnamen des Superusers, und das zugehörige Kennwort ein.

Verfeinertes Ereignis

Ein *verfeinertes Ereignis* sind zugeordnete oder verfeinerte Ereignisdaten, die von einem Rohereignis oder von zusammengefassten Ereignissen stammen. CA Enterprise Log Manager führt die Zuordnung und Analyse aus, damit die gespeicherten Informationen durchsucht werden können.

Verfügbarmachung

Die *Verfügbarmachung* bezeichnet die Statusänderung einer Datenbank von "kalt" in "verfügbar gemacht". Der Prozess wird von CA Enterprise Log Manager durchgeführt, wenn dieser vom Hilfsprogramm "LMArchive" benachrichtigt wird, dass eine bekannte kalte Datenbank wiederhergestellt wurde. (Wenn die kalte Datenbank nicht auf ihrem ursprünglichen CA Enterprise Log Manager wiederhergestellt wird, das Hilfsprogramm "LMArchive" nicht verwendet wird und eine Verfügbarmachung nicht erforderlich ist, wird die wiederhergestellte Datenbank bei der Neukatalogisierung als warme Datenbank hinzugefügt.)

Vernetzte Föderation

Eine *Vernetzte Föderation* von CA Enterprise Log Manager-Servern ist eine Topologie, die eine gleichartige Beziehung zwischen Servern einrichtet. In seiner einfachsten Form ist dies der Fall, wenn Server 2 ein untergeordneter Server von Server 1 ist und umgekehrt. Ein vernetztes Paar von Servern hat eine Beziehung, die in beide Richtungen geht. Eine vernetzte Föderation kann so definiert werden, dass viele Server alle untereinander gleichrangig sind. Eine föderierte Abfrage gibt die Ergebnisse vom ausgewählten Server und all seinen gleichrangigen Servern zurück.

Verwaltung von Berechtigungen

Die *Verwaltung von Berechtigungen* ist ein Mittel zur Steuerung der Aktionen, die Benutzer durchführen dürfen, sobald sie sich authentifiziert und an der CA Enterprise Log Manager-Oberfläche angemeldet haben. Dies geschieht über Zugriffsrichtlinien, die mit den Rollen, die den Benutzern zugewiesen wurden, verknüpft werden. Rollen, oder Anwendungsbenutzergruppen, und Zugriffsrichtlinien können vordefiniert oder benutzerdefiniert sein. Die Verwaltung von Berechtigungen wird über den internen CA Enterprise Log Manager-Benutzerspeicher gehandhabt.

Visualisierungskomponenten

Visualisierungskomponenten sind verfügbare Optionen, mit denen Berichtsdaten einschließlich Tabelle, Diagramm (Zeilendiagramm, Balkendiagramm, Spaltendiagramm, Kreisdiagramm) oder ein Ereignis angezeigt werden können.

Wiederherstellungspunkt-Server

Ein *Wiederherstellungspunkt-Server* ist eine Rolle, die von einem CA Enterprise Log Manager-Server ausgeführt wird. Um "kalte" Ereignisse zu untersuchen, können Sie Datenbanken mit einem Hilfsprogramm vom Remote-Speicher zum Wiederherstellungspunkt-Server verschieben, dann die Datenbanken zum Katalog hinzufügen und Abfragen durchführen. Das Verschieben kalter Datenbanken zu einem bestimmten Wiederherstellungspunkt-Server ist eine alternative Methode dazu, sie aus Untersuchungsgründen zurück zum ursprünglichen Server zu verschieben.

XMP-Dateianalyse

XMP-Dateianalyse ist der Prozess, der vom Nachrichtenanalyse-Hilfsprogramm durchgeführt wird, um alle Ereignisse zu suchen, die jede vorabgestimmte Zeichenfolge enthalten, und um bei einem übereinstimmendem Ereignis das Ereignis mit dem ersten gefundenen Filter, der dieselbe vorabgestimmte Zeichenfolge verwendet, in Tokens zu analysieren.

Zertifikate

In CA Enterprise Log Manager werden die vordefinierten *Zertifikate* "CAELMCert.p12" und "CAELM_AgentCert.p12" verwendet. Alle CA Enterprise Log Manager-Services verwenden zur Kommunikation mit dem Verwaltungsserver das Zertifikat "CALEMCert.p12". Alle Agenten verwenden zur Kommunikation mit dem zugehörigen Erfassungsserver das Zertifikat "CAELM_AgentCert.p12".

Zugriffsfilter

Ein *Zugriffsfilter* kann vom Administrator festgelegt werden, um zu steuern, welche Ereignisdaten Benutzer oder Gruppen ohne Administratorrechte anzeigen können. So kann ein Zugriffsfilter beispielsweise den Datenumfang in Berichten einschränken, der von bestimmten Identitäten eingesehen werden kann. Zugriffsfilter werden automatisch in Pflichtrichtlinien konvertiert.

Zugriffsrichtlinie

Eine *Zugriffsrichtlinie* ist eine Regel, die einer Identität (Benutzer oder Benutzergruppe) Zugriffsrechte auf eine Anwendungsressource gewährt oder verweigert. CA Enterprise Log Manager bestimmt anhand der Übereinstimmung von Identitäten, Ressourcen, Ressourcenklassen und der Auswertung der Filter, welche Richtlinien für einen bestimmten Benutzer gelten.

Zugriffssteuerungsliste für Identitäten

Mit der *Zugriffssteuerungsliste für Identitäten* können Sie verschiedene Aktionen angeben, die ausgewählten Identitäten in ausgewählten Ressourcen gewährt werden sollen. Beispielsweise können Sie mit der Zugriffssteuerungsliste für Identitäten angeben, dass eine Identität Berichte erstellen und eine andere Berichte planen und anmerken kann. Eine Zugriffssteuerungsliste für Identitäten unterscheidet sich darin von einer Zugriffssteuerungsliste, dass sie sich auf Identitäten und nicht auf Ressourcen richtet.

Zuordnungsanalyse

Eine *Zuordnungsanalyse* ist ein Schritt im Assistenten zur Dateizuordnung, bei dem Sie eine Datenzuordnungsdatei testen und ändern können. Beispielereignisse werden mit der Datenzuordnungsdatei verglichen, und die Ergebnisse werden mit CEG geprüft.

Zusammenfassungsregeln

Zusammenfassungsregeln fassen bestimmte gängige, native Ereignistypen zu einem verfeinerten Ereignis zusammen. Eine Zusammenfassungsregel kann beispielsweise so konfiguriert werden, dass sie bis zu 1000 doppelte Ereignisse, die dieselben Quell- und Ziel-IP-Adressen und Ports haben, durch ein Zusammenfassungsereignis ersetzt. Diese Regeln vereinfachen die Ereignisanalyse und verringen das Protokollaufkommen.

Index